Administering TC endpoints on CUCM8.6

QUICK START GUIDE

- Cisco Unified Communications Manager 8.6
- Cisco TelePresence MX Series
- Cisco TelePresence EX Series
- Cisco TelePresence Codec C Series
- Cisco TelePresence Profile Series
- Cisco TelePresence Quick Set C20

Software versions TC5.0 and Cisco Unified Communications Manager 8.6
November 2011

Thank you for choosing Cisco TelePresence!

Your Cisco product has been designed to give you many years of safe, reliable operation.

This part of the product documentation is aimed at administrators working with the setup of the TelePresence endpoints on Cisco Unified Communications Manager 8.6.

Our main objective with this guide is to address your goals and needs. Please let us know how well we succeeded! Go to the feedback page, click here...

May we recommend that you visit the Cisco web site regularly for updated versions of this guide.

The user documentation can be found on ▸ http://www.cisco.com/go/telepresence/docs.

How to use this guide

The top menu bar and the entries in the Table of contents are all hyperlinks. You can click on them to go to the topic.

Table of contents

Chapter 1

Prerequisites

Prerequisites

This document is a quick guide with the information required to deploy Cisco TelePresence endpoints on the Cisco Unified Communications Manager.

Products covered by this guide

- Cisco Unified Communications Manager – CUCM 8.6
- Cisco TelePresence MultiPoint Switch - CTMS 1.8
- Cisco TelePresence Manager - CTS-MAN 1.8
- Cisco TelePresence products – TC 5.0
  - MX200
  - MX300
  - EX90
  - EX60
  - Codec C90
  - Codec C60
  - Codec C40
  - Profiles with Codec C Series
  - Quick Set C20

Load the correct versions of the software

Before you start configuring, make sure the endpoints and CUCM have the correct software installed.

- CUCM version 8.6.1.10000-43 or higher. To add Profile 42 (C40) and MX Series models and to enable CTI monitoring support for CTS-Manager use 8.6(2) or later. Optionally use 8.6(1) with a device pack from December 2011 or later.
- EX-/C-/MX-Series version TC5. Note that the C20 must have high definition/premium resolution option to interoperate with CTMS.
- CTMS version 1.8 or higher.
- CTS-MAN version 1.8 or higher.

Chapter 2

TelePresence Endpoint Configuration

TelePresence endpoint configuration

The TelePresence endpoint configuration is done in three steps.

Step 1

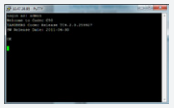
If required: Reset the TelePresence endpoint to factory defaults

If the codec has been used with TMS or a similar system, then a Factory reset must be carried out first. In cases where the codec is new and unused, a Factory reset will not be needed. When resetting the codec to factory default this will be followed by an automatic reboot of the codec. The call logs will be deleted and all system parameters will be reset to default values. All files that have been uploaded to the codec will be deleted. The Release key and Option key will not be affected.

If you are moving the endpoint from TMS to CUCM then remove the endpoint from TMS and disable TMS' ability to automatically detect devices.

Choose one of the following methods to reset the endpoint to factory defaults:

Touch interface  Read more..

API command  Read more..

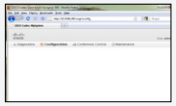
Step 2

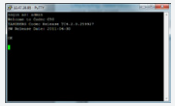
Set the provisioning mode

Choose one of the following methods to set the provisioning mode:

Touch interface  Read more..

OSD/Remote control  Read more..

Web interface  Read more..

API command  Read more..

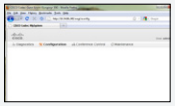
Step 3

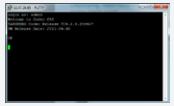
Set the default call rate

Choose one of the following methods to set the default call rate:

Touch interface  Read more..

OSD/Remote control  Read more..

Web interface  Read more..

API command  Read more..

Resetting the TelePresence endpoint to factory defaults using the Touch interface

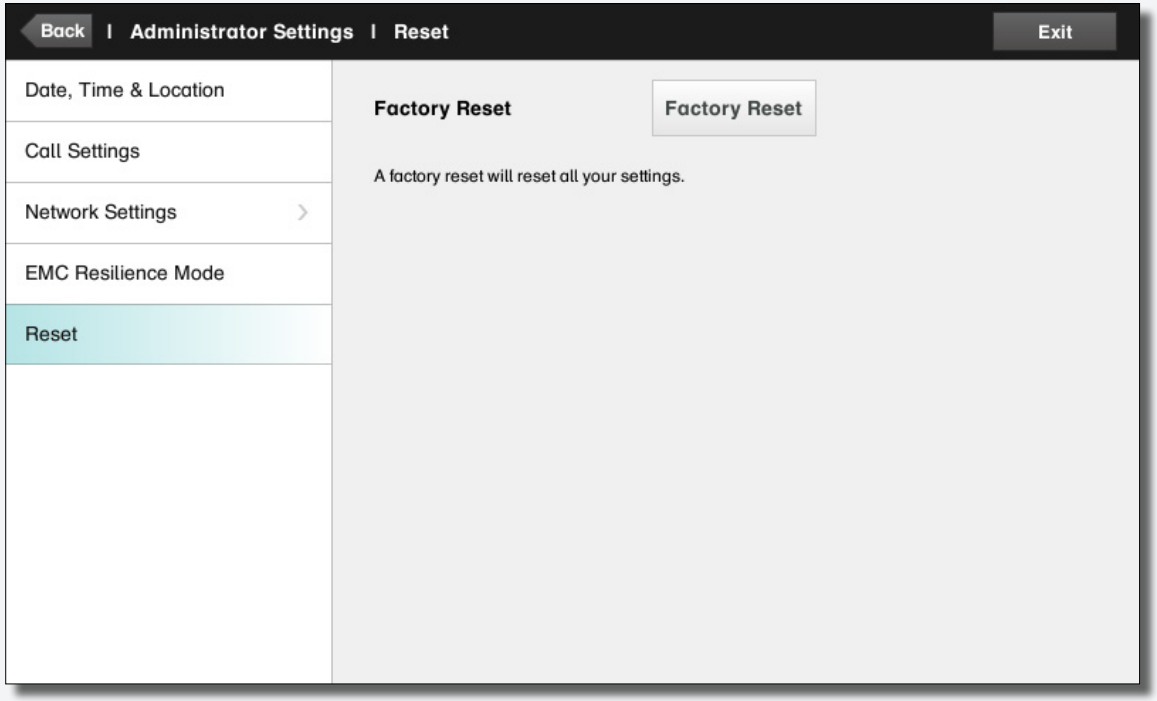
NOTE: If the codec has been used with TMS or a similar system, then a Factory reset must be carried out first. In cases where the codec is new and unused, a Factory reset will not be needed. When resetting the codec to factory default this will be followed by an automatic reboot of the codec. The call logs will be deleted and all system parameters will be reset to default values. All files that have been uploaded to the codec will be deleted. The Release key and Option key will not be affected.

If you are moving the endpoint from TMS to CUCM then remove the endpoint from TMS and disable TMS' ability to automatically detect devices.

If required: Resetting the endpoint to factory defaults

1. If the unit is in sleep mode, then tap gently on the touch panel to wake up the Touch.
2. Select More..
3. Select Settings
4. Select Administrator Settings
5. Select Reset and press the **Factory Reset** button
6. The codec will automatically reboot, reverting to the default factory settings. This will take a few minutes.

Step 1 (if required)



Back to overview

Setting the provisioning mode using the Touch interface

Setting the provisioning mode

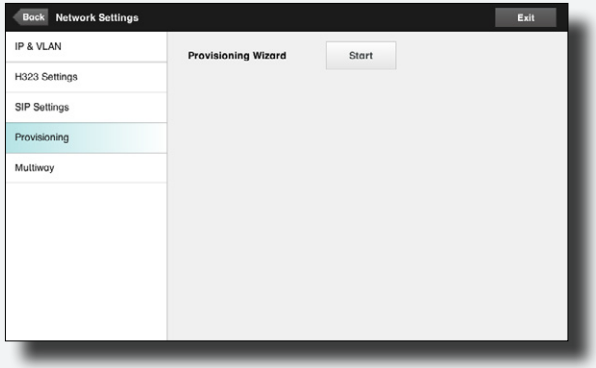
1. Select More..
2. Select Settings
3. Select Network Settings
4. Select Provisioning
5. Start the Provisioning Wizard

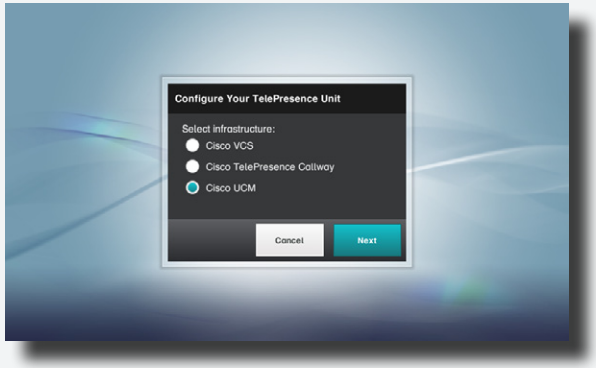
Follow the instructions in the Provisioning Wizard

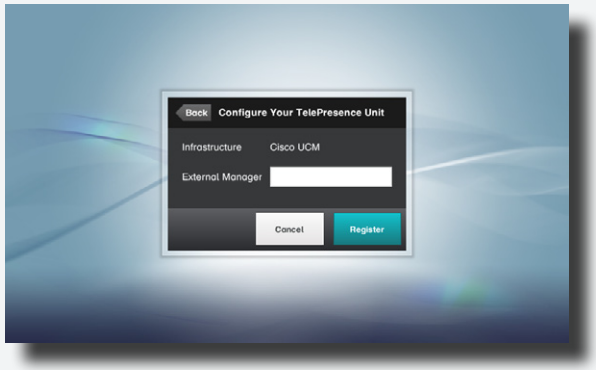
1. Set the infrastructure to **Cisco UCM** and select **Next**.
2. The Provisioning Wizard will prompt you for the External Manager address. Enter the address of the UC Manager TFTP server.
3. Select **Register** to initiate the Cisco UCM registering.

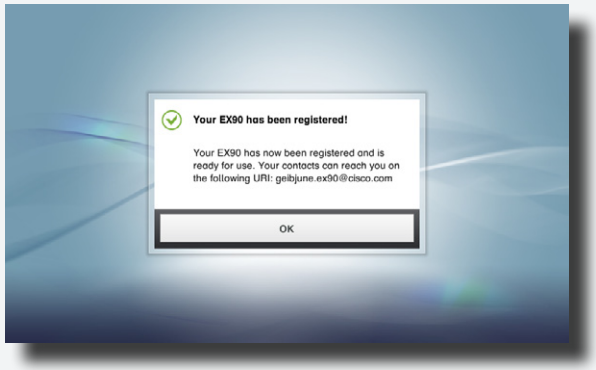
NOTE: When set to Cisco UCM; CDP will be enabled and if CDP is successful, then the endpoints will discover DHCP Option 150. If the network does not offer DHCP Option 150, then the IP Address of the external manager must be added manually.

Step 2









Back to overview

Setting the default call rate using the Touch interface

Setting the provisioning mode

1. Select More..
2. Select Settings
3. Select Adminisrator Settings
4. Select Call Settings and set the **Default Call Rate**.

NOTE: For deployment with CTMS, the recommended value is 2500kbps or higher.

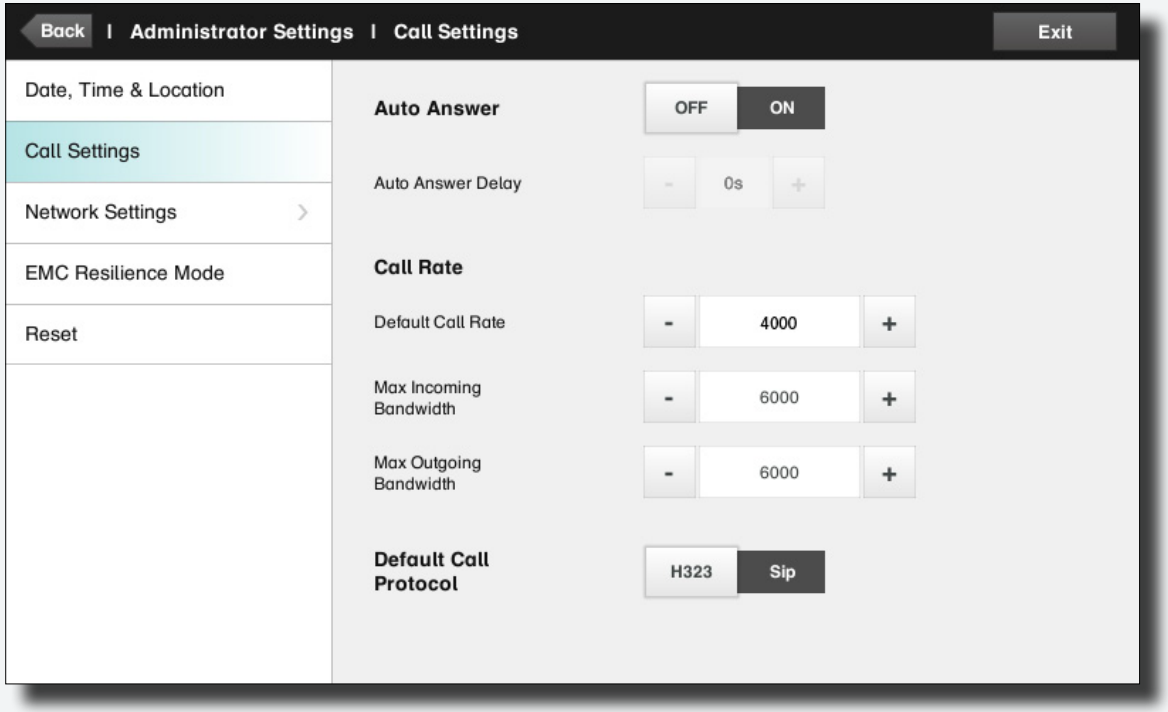
About the Auto Answer setting

The Auto Answer setting provisioned in UC Manager Administration is ignored by the endpoint in TC5.0.0. Consequently, it must be set on the endpoint itself.

About the Default Call Protocol setting

In CUCM mode the default protocol is automatically set to SIP and H.323 is not supported.

Step 3



Note how the settings chosen are indicated. In the example shown, Auto Answer is set to On and the Default Call Protocol is set to SIP.

Back to overview

Setting the provisioning mode using the OSD/Remote Control

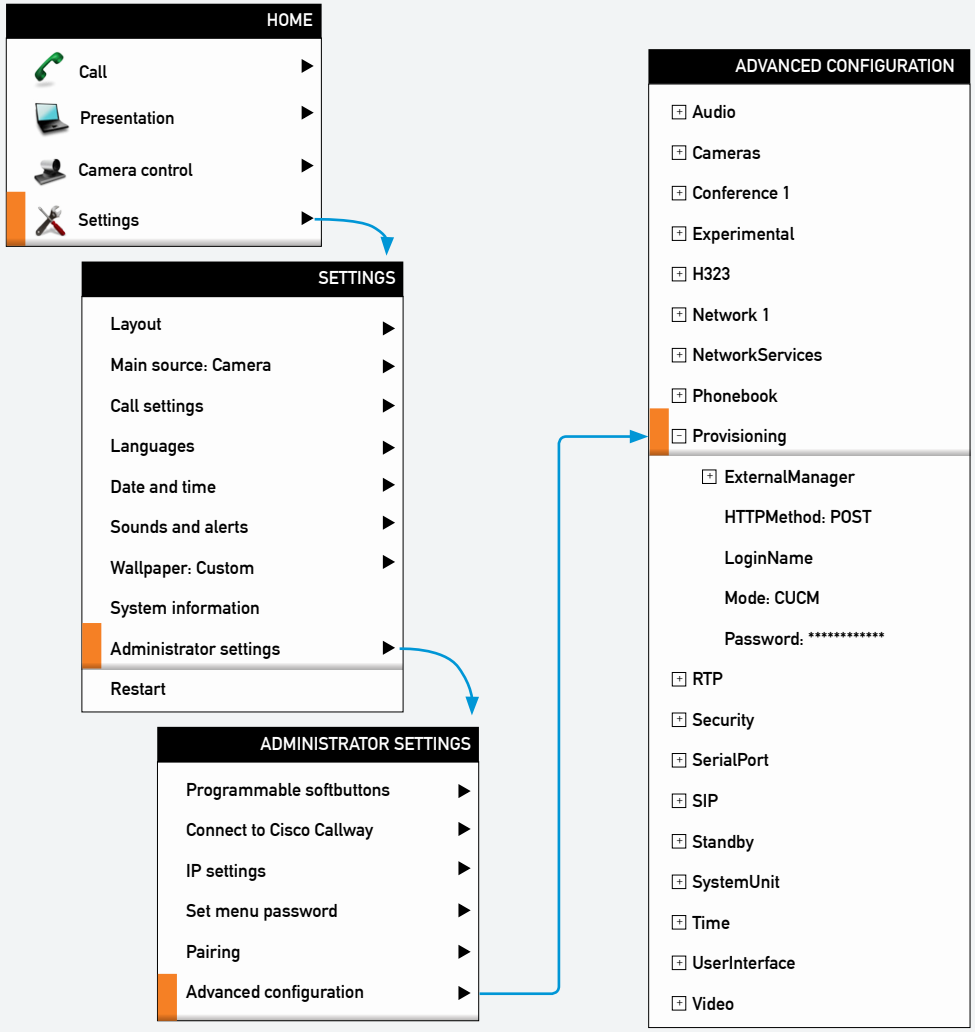
Setting the provisioning mode

1. If the codec has been used with TMS or a similar system, then a Factory reset must be carried out first, see "Resetting the TelePresence endpoint to factory defaults using the API interface" on page 14. In cases where the codec is new and unused, a Factory reset will not be needed.

   If you are moving the endpoint from TMS to CUCM then remove the endpoint from TMS and disable TMS' ability to automatically detect devices.
2. If the system is in sleep mode, then press any key on the remote control to wake up the system.
3. Select Home
4. Select Settings
5. Select Administrator Settings
6. Select Advanced Configuration
7. Select Provisioning and set the **Provisioning Mode** to **CUCM**
8. The change will take effect immediately.

NOTE: If CDP is enabled and successful, then the endpoints will discover DHCP Option 150. If the network does not offer DHCP Option 150, then the IP Address of the external manager must be added manually.

Step 2



Back to overview

Setting the default call rate using the OSD/Remote Control

Setting the default call rate mode

1. If the system is in sleep mode, then press any key on the remote control to wake up the system.
2. Select Home
3. Select Settings
4. Select Administrator Settings
5. Select Advanced Configuration
6. Select Conference
7. Select DefaultCall and set the **Rate** to the appropriate value (kbps).

   NOTE: For deployment with CTMS, the recommended value is 2500 kbps or higher.
8. The change will take effect immediately.

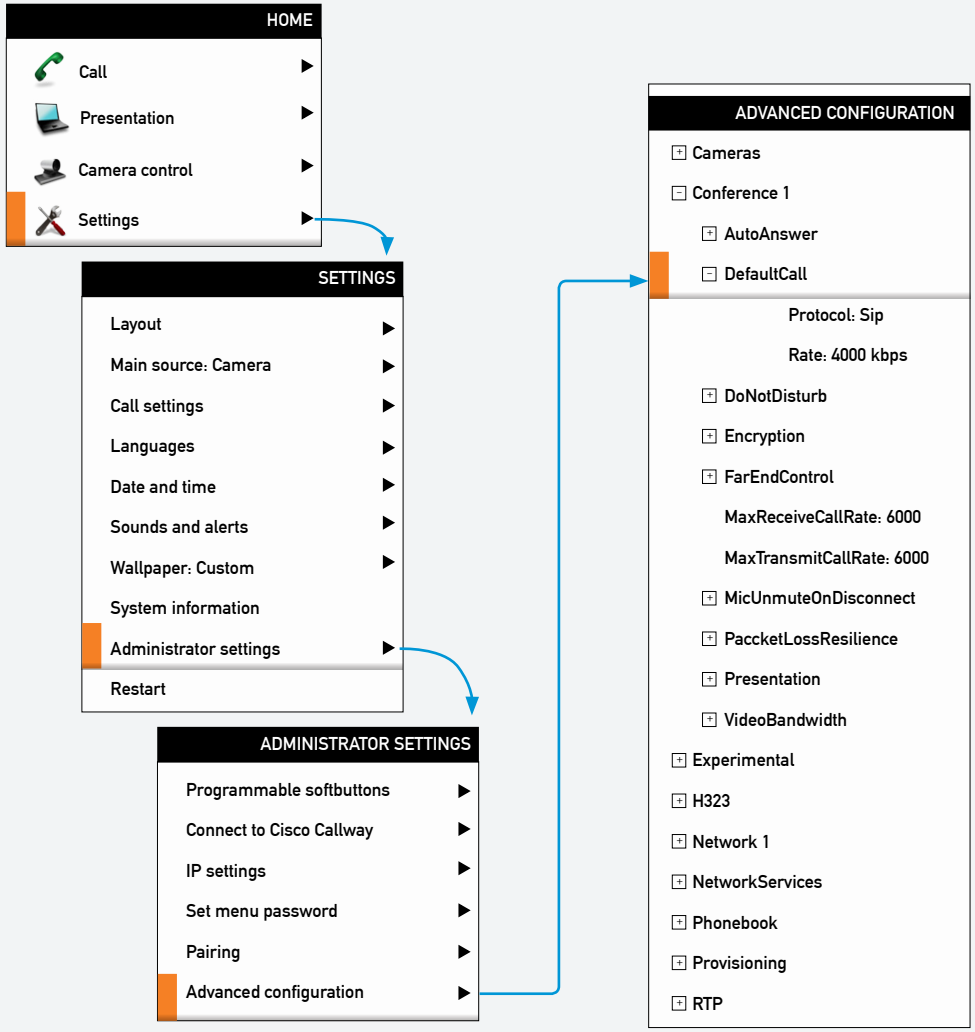
About the Auto Answer setting

The Auto Answer setting provisioned in UC Manager Administration is ignored by the endpoint in TC5.0.0 and therefore must be set locally on the endpoint itself.

About the Default Call Protocol setting

In CUCM mode the default protocol is automatically set to SIP and H.323 is not supported.

Step 3



Back to overview

Setting the provisioning mode using the Web interface

Setting the provisioning mode

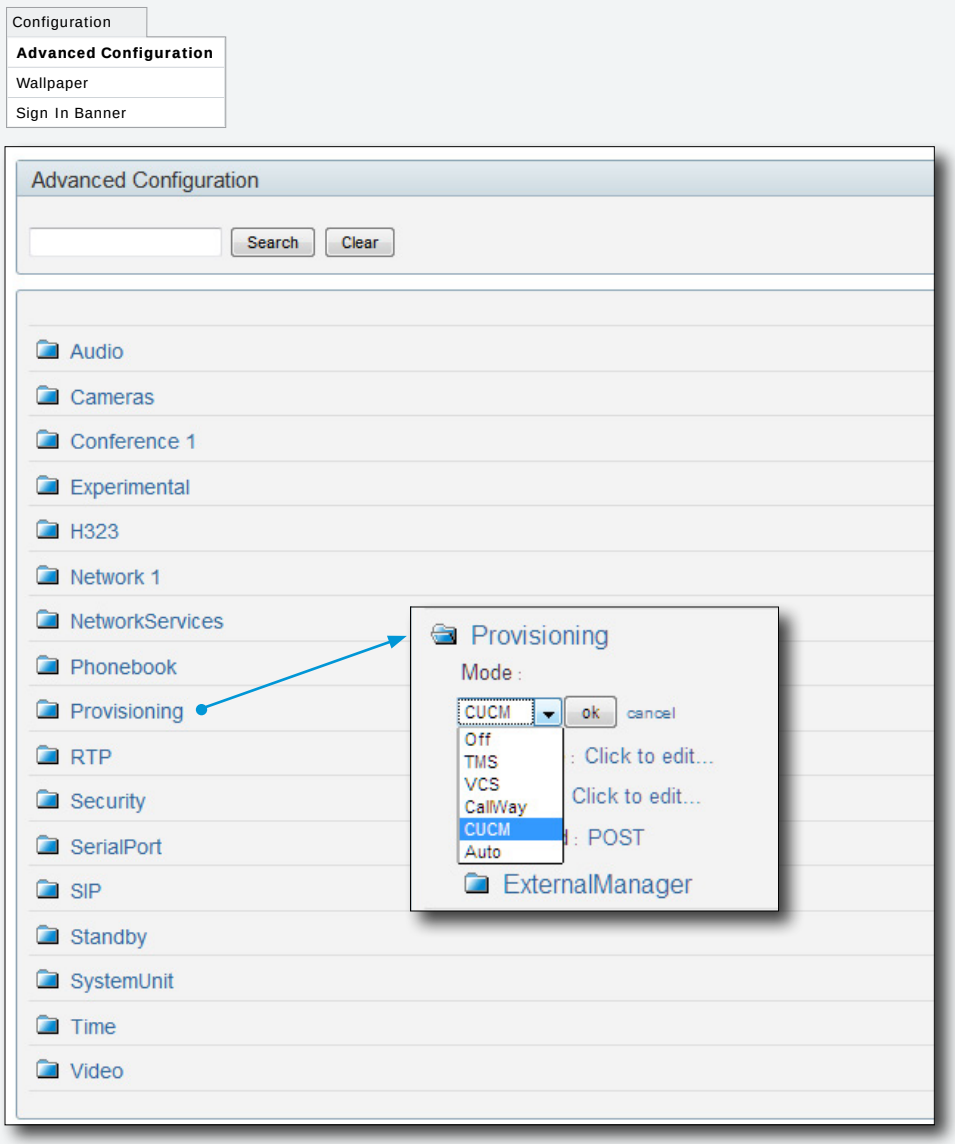
1. If the codec has been used with TMS or a similar system, then a Factory reset must be carried out first, see "Resetting the TelePresence endpoint to factory defaults using the API interface" on page 14. In cases where the codec is new and unused, a Factory reset will not be needed.

   If you are moving the endpoint from TMS to CUCM then remove the endpoint from TMS and disable TMS' ability to automatically detect devices.

2. Open a web browser and enter the IP address to connect to the video system. Enter the user name. If a password has been set, enter the password.
3. Select **Configuration** from the top menu.
4. Select **Advanced Configuration** from the drop down list.
5. Select Provisioning and set the **Provisioning Mode** to CUCM
6. Press the **OK** button to make the change take effect.

NOTE: If CDP is enabled and successful, then the endpoints will discover DHCP Option 150. If the network does not offer DHCP Option 150, then the IP Address of the external manager must be added manually.

Step 2



Back to overview

Setting the default call rate using the Web interface

Setting the default call rate mode

1. If not already logged in, then open a web browser and enter the IP address to connect to the video system. Enter the user name. If a password has been set, then enter the password.
2. Select **Configuration** from the top menu.
3. Select **Advanced Configuration** from the drop down list.
4. Select **Conference 1**
5. Select **DefaultCall** and set the Rate to the appropriate value (kbps).

   NOTE: For deployment with CTMS, the recommended value is 2500 kbps or higher.
6. Press the **OK** button to make the change take effect.

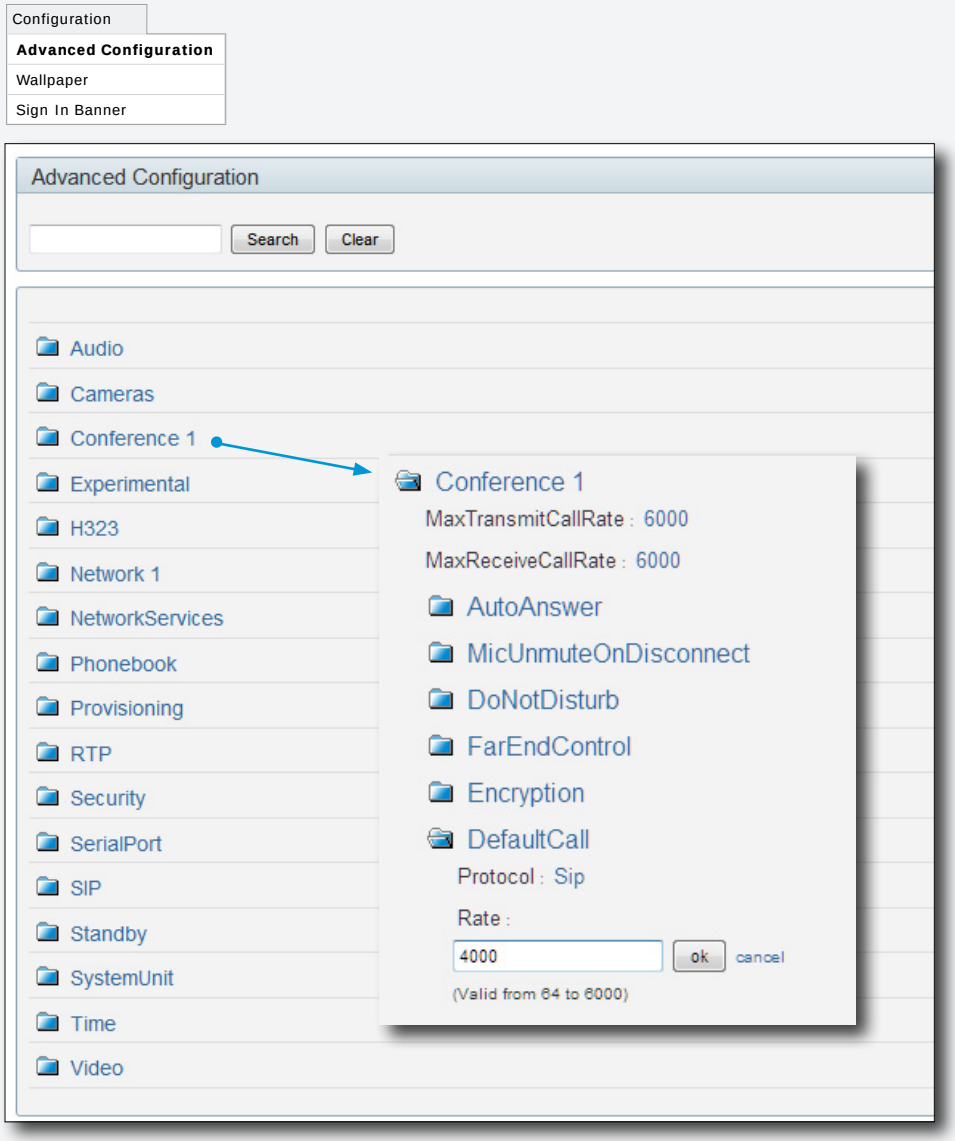
About the Auto Answer setting

The Auto Answer setting provisioned in UC Manager Administration is ignored by the endpoint in TC5.0.0. Consequently, it must be set on the endpoint itself.

About the Default Call Protocol setting

In CUCM mode the default protocol is automatically set to SIP and H.323 is not supported.

Step 3



Back to overview

Resetting the TelePresence endpoint to factory defaults using the API interface

If the codec has been used with TMS or a similar system, then a Factory reset must be carried out first. In cases where the codec is new and unused, a Factory reset will not be needed.

Step 1 (if needed)

xCommand SystemUnit FactoryReset

Reset the codec to factory default settings. This action is followed by an automatic reboot of the codec. The call logs will be deleted and all system parameters will be reset to default values. All files that have been uploaded to the codec will be deleted. The Release key and Option key will not be affected.

Requires user role: ADMIN

Parameters: Confirm(r): <Yes>

Example: `xCommand SystemUnit FactoryReset Confirm: Yes`

```
*r FactoryResetConfirmResult (status=OK):
** end
```

Back to overview

Configuring the provisioning settings using the API interface

Configure the provisioning settings

Configure the Provisioning settings:

- `xConfiguration Provisioning Mode: [must be CUCM]`
- `xConfiguration Provisioning ExternalManager Address: [CUCM cluster TFTP server address]`
- `xConfiguration Provisioning ExternalManager Protocol: [must be HTTP for UCM mode]`
- `xConfiguration Provisioning LoginName: [leave blank...not needed for UCM mode]`
- `xConfiguration Provisioning Password: [leave blank...not needed for UCM mode]`
- `xConfiguration Provisioning HttpMethod: [both GET and POST work in UCM mode]`
- `xConfiguration Provisioning ExternalManager Path: [leave blank...not needed for UCM mode]`
- `xConfiguration Provisioning ExternalManager Domain: [leave blank...not needed for UCM mode]`

NOTE: If CDP is enabled and successful, then the endpoints will discover DHCP Option 150. If the network does not offer DHCP Option 150, then the IP Address of the external manager must be added manually.

Back to overview

Step 2

xConfiguration Provisioning Mode

Provides the possibility of managing the codec (endpoint) by using an external manager/management system. Contact your Cisco representative if you need more information on the different options.

Requires user role: ADMIN

Value space: <Off/TMS/VCS/CallWay/CUCM/Auto>

Off: The system will not try to register to any management system.
TMS: If set to TMS (Cisco TelePresence Management System) then the system will try to register to a TMS server.
VCS: If set to VCS (Cisco TelePresence Video Communication Server) then the system will try to register to a VCS.
Callway: If set to Callway then the system will try to register to the Callway subscription provider.
CUCM: If set to CUCM (Cisco Unified Communications Manager) then the system will try to register to a CUCM.
Auto: The provisioning server will automatically be selected by the system.

Example: `xConfiguration Provisioning Mode: CUCM`

xConfiguration Provisioning ExternalManager Address

Enter the IP Address to the External Manager/Management system. If an External Manager address and a path is configured, then the system will post an HTTP message to this address when starting up. When receiving this HTTP posting the External Manager (typically a management system) can return configurations/commands to the unit as a result. If the DHCP Option 242 is returned in the DHCP response from the DHCP server then the system will interpret this as the External Manager address to use.

Requires user role: ADMIN

Value space: <S: 0, 64>

Format: Only the valid IP address format is accepted. An IP address that contains letters (192.a.2.0) or unvalid IP addresses (192.0.1234.0) will be rejected.

Example: `xConfiguration Provisioning ExternalManager Address: “”`

xConfiguration Provisioning ExternalManager Protocol

Determine whether or not to use secure management.

Requires user role: ADMIN

Value space: <HTTP/HTTPS>

HTTP: Set to HTTP to disable secure management. Requires HTTP to be enabled in the xConfiguration NetworkServices HTTP Mode setting.
HTTPS: Set to HTTPS to enable secure management. Requires HTTPS to be enabled in the xConfiguration NetworkServices HTTPS Mode setting.

Example: `xConfiguration Provisioning ExternalManager Protocol: HTTP`

Setting the default call rate using the API interface

Setting the default call rate

Set the default call rate.

- `xConfiguration Conference 1 DefaultCall Rate`

For deployment with CTMS, the recommended value is 2500 kbps or higher.

About the Auto Answer setting

The Auto Answer setting provisioned in UC Manager Administration is ignored by the endpoint in TC5.0.0 and therefore must be set locally on the endpoint itself.

About the Default Call Protocol setting

In CUCM mode the default protocol is automatically set to SIP and H.323 is not supported.

Step 3

xConfiguration Conference [1..1] DefaultCall Rate

Set the default call rate to be used when placing calls from the system.

Requires user role: ADMIN

Value space: <64..6000>

Range: Select a value between 64 and 6000 kbps

Example: `xConfiguration Conference 1 DefaultCall Rate: 4000`

Back to overview

Chapter 3

CUCM configuration

Configuring the Cisco Unified Communications Manager 8.6

1. If you are moving the endpoint from TMS to CUCM then remove the endpoint from TMS and disable TMS's ability to automatically detect devices.

2. Select the endpoint model from the drop down list

Select: "Cisco TelePresence [EX|MX|Profile|Cx0" model.

3. Setting the CUCM registration mode

In UCM Administration

Either enable Auto-Registration, or manually configure your endpoints by MAC address.

4. Configuring the SIP Profile

In UCM Administration > Device > Device Settings > SIP Profile

Create a new SIP Profile.
Hint: Copy the existing Default SIP Profile to create a new one.

- Enable "Redirect by Application" for call forward all.
- Set "SDP Session-level Bandwidth Modifier for Early Offer and Re-invites" to TIAS and AS.
- Enable "Use Fully Qualified Domain Name in SIP Requests".
- If not already set; then enable "Allow Presentation Sharing using BFCP".

Assign this SIP Profile to all MX, EX and C-Series endpoints.

5. Setting the Organizational Top Level Domain

In UCM Administration > System > Enterpice Parameters

Set the Organizational Top Level Domain, e.g. cisco.com

6. Setting the Regions and Locations

In UCM Administration > System [Region | Location]

Configure Regions and Locations to permit the appropriate bandwidth.

- 128 kbps (AAC-LD [LATM]).
- 4000 kbps video. NOTE: 2500 kbps or higher is recommended for deployments with CTMS.
- For MultiSite capable units the location settings needs to reflect the maximum number of simultaneous calls.

7. Setting the Calling Search Spaces, Prtitions and Presence Permissions

In UCM Administration

Assign Calling Search Spaces, Partitions and Presence permissions to the devices as appropriate. For the MX, EX and C-Series endpoints set the Redirecting Calling Search Spaces for call transfer and Call Forward All.

8. Setting the DCSP Parameters

In UCM Administration

Set the DSCP parameters according to your network. Here are the default values:

- DSCP for Phone-based Services: Default DSCP 000000
- DSCP for Phone Configuration: CS3 (precedence 3) DSCP (011000)
- DSCP for UCM to Device Interface: CS3 (precedence 3) DSCP (011000)
- DSCP for Audio Calls: EF DSCP (101110)
- DSCP for Video Calls: AF41 DSCP (100010)
- DSCP for TelePresence Calls: CS4 (precedence 4) DSCP (100000)

9. Setting a NTP Reference for the endpoints

In UCM Administration > System > NTP Reference

Configure a Phone NTP Reference for the endpoints.

- The NTP Reference must be in Unicast Mode.
- Assign to Date/Time Group, which in turn is assigned to Device Pool.

10. Setting up the UCM Services

In UCM Administration > Serviceability -> Tools -> Service Activation

Enable the necessary UCM Services

- Cisco CallManager
- Cisco IP Voice Media Streaming App
- Cisco User Data Services (must be enabled on the node the endpoints are registering to). The MX, EX and C Series endpoints uses this for the phone book.
- Cisco Tftp
- Others as desired

Configuring the Cisco Unified Communications Manager Interop

When deployed with CTMS, make sure to set the CTMS in interop mode. See CTMS 1.8 documentation.

Product Specific Configuration Layout

Configure the product specific configuration layouts.

In UCM Administration > Device -> Phone -> [selected endpoint] -> Product Specific Configuration section

Room Name (from Exchange(R)):

This is the Exchange Conference Room Name. It is used for scheduling meetings where this TelePresence system participates. (NOTE: This setting must match the email address used in Exchange exactly) e.g. room123@cisco.com.

- Maximum length: 64

Web Access:

This parameter indicates whether the device will accept connections from a web browser or other HTTP client. Disabling the web server functionality of the device will block access to the phone's internal web pages and certain support capabilities, but will not degrade normal operation. A device RESET is required for this parameter to take effect.

- Default: Disabled

NOTE! For this Web Access config change to take effect, please make sure to **Save** and **RESET** the device (**not** Restart or Apply Config).

SSH Access:

This parameter indicates whether the device will accept ssh connections. Disabling the ssh server functionality of the device will block certain support capabilities such as log file collection but will not degrade normal operation.

- Default: Disabled

Default Call Protocol:

This parameter sets the default call protocol of the device. This device only supports SIP when registering to Cisco Unified Communications Manager.

- Default: SIP

Quality Improvement Server:

Specifies a hostname or IP address of a remote system to collect quality improvement reports from the device.

- Default: “”
- Maximum length: 256

Admin username and password

Configure the username and password. This is required for CTS-Manager to discover the endpoints and provide One Button to Push scheduling to them.

Admin Username:

Enter a user ID for the admin user

- Default: admin
- Maximum length: 64
- Allowed values: Admin username cannot be one of apache, daemon, nobody, root, shutdown. It must be between 1 and 64 characters long.

Admin Password:

Enter the password for the admin user

- Default: “”
- Maximum length: 64
- Allowed values: Admin password can only contain printable characters from the ASCII charset, except whitespace.

NOTE! User name and password will not be pushed to the equipment, you must set it yourself.

Dial Plan

Configure the dial plan. Refer to CTS-Manager documentation for more details.

Directory Number

Configure the directory number. Refer to CTS-Manager documentation for more details.

Chapter 4

Appendices

Password administration for the endpoints

You need a username and password to sign in to the web and command line interfaces of your system.

The TelePresence system is delivered with a default user account with username admin and no password set. This user has full access rights to the system.

NOTE: We strongly recommend that you set a password for the admin user to restrict access to system configuration.

Make sure to keep a copy of the password in a safe place. You will have to contact your Cisco representative if you have forgotten the password.

NOTE: The admin password set on the endpoint must match the value set in UC Manager Product Specific Configuration Layout in order for CTS-Manager to discover the endpoints and provide One Button to Push scheduling to them. You must do this manually.

Changing the system password

Perform the following steps to change the system password.

If no password currently is set, then use a blank *Current password*; to remove a password, leave the *New password* fields blank.

1. Sign in to the web interface with your username and current password.
2. Go to the *Maintenance* tab and select *Change Password*.
3. Enter the *Current password*, the *New password*, and repeat the new password in the appropriate input fields.

   The password format is a string with 0–64 characters.
4. Click *Change password*.

Changing another user's system password

Read more about creating more user accounts in the ▸ User management section.

If you have ADMIN rights, you can change all users' passwords by performing the following steps:

1. Sign in to the web interface with your username and password.
2. Go to the *Maintenance* tab and select *User administration*.
3. Select the appropriate user from the list.
4. Enter a new password and PIN code.
5. Click *Save*.

Setting the Administrator settings menu password

When starting up the system for the first time the Administrator Settings menu password is not set.

NOTE: We strongly recommend that you define a password to protect the Administrator Settings menu on the Touch controller, since these settings affect the behavior of the video conference system.

You need to use a command line interface to set the Administrator Settings menu password; you neither can use the Touch controller nor the web interface.

Setting the Administrator Settings menu password

1. Connect to the system through the network or the serial data port, using a command line interface (SSH or Telnet).
2. Type the following command:

   ```
   xCommand SystemUnit MenuPassword Set
   Password: <password>
   ```

   The password format is a string with 0–255 characters.

Setting a root password

You can also protect the file system of your video system by setting a password for the root user. The root user is disabled by default. You have to use the command line interface to enable the root user and set a root password.

Setting a root password

Perform the following steps to activate the root user and set a password for it:

1. Connect to the system through the network or the serial data port, using a command line interface (SSH or Telnet).
2. Sign in to the system with username and password. The user needs ADMIN rights.
3. Type the following command:

   ```
   systemtools rootsettings on <password>
   ```

NOTE: The root password is not the same as the system (admin) password.

Understanding Cisco Discovery Protocol on the former TANDBERG endpoints

Introduction

Cisco Discovery Protocol (CDP) is a proprietary layer-2 management protocol developed by Cisco in the early 1990s to provide enhanced automation of network discovery and management. It is broadly deployed on millions of existing Cisco products and provides countless benefits to network administrators for managing router and switch interfaces. With the introduction of IP Telephony in the late 1990s and early 2000s, CDP was enhanced to provide additional automation capabilities for IP-based telephones, including automatic VLAN discovery, Power over Ethernet (POE) negotiation, Quality of Service (QoS) automation, location awareness (to automate the discovery of the physical location of an IP telephone for management and emergency services purposes), Ethernet speed and duplex mismatch detection, and more.

Note: The IETF, IEEE and TIA, in cooperation with Cisco and numerous other networking vendors, have since created the IEEE 802.1AB standard, known as Link-Layer Discovery Protocol (LLDP), with extensions developed for Media Endpoint Discovery (LLDP-MED) for voice and video endpoints. LLDP-MED will eventually subsume CDP, but this may take years to unfold due to the enormous installed-base and widespread use of CDP.

Cisco acquired TANDBERG in April 2010. The TANDBERG portfolio of video endpoints compliments Cisco's existing Telepresence and Unified Communications solutions. CDP support was introduced on the Cisco E20 in release TE4.0, and is introduced on the Cisco TelePresence MX series, EX series, Codec C Series, Profile series and Quick Set C20, in release TC5.0.

However, because there is already an installed-base of these endpoint models (prior to the Cisco acquisition) that are not running CDP, introducing CDP in a software release requires careful consideration of how the new automation functionality will affect that existing installed-base. Enabling CDP by default could cause undesired behavior for those existing deployments when they upgrade to a CDP-enabled release and the devices suddenly begin using VLAN automation, so CDP is being introduced in a phased approach.

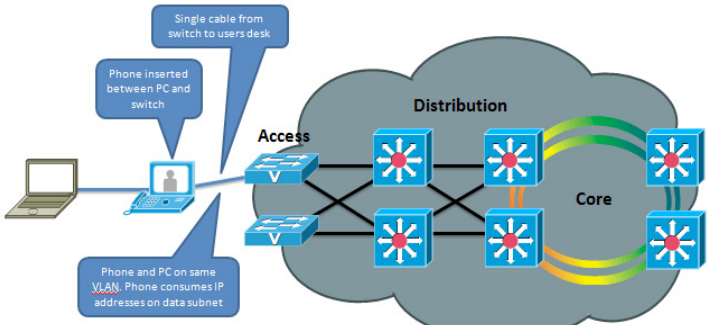


Figure 1: Without VLANs

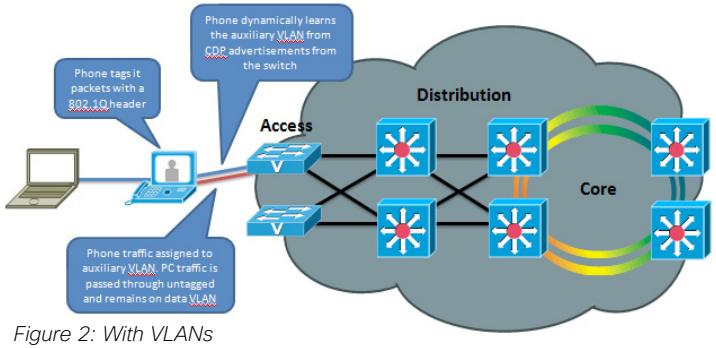


Figure 2: With VLANs

Benefits Provided by CDP

As mentioned in the introduction above, CDP provides numerous automation benefits for network administrators deploying IP-based voice and video endpoints on their networks. This section briefly highlights some of the most pertinent benefits for IP-based voice/video endpoints like the Cisco TelePresence MX series, EX series, Codec C Series, Profile series and Quick Set C20.

Automatic VLAN discovery

Virtual LANs (VLANs) allow a network administrator to introduce IP-based telephones and video terminals onto their network without the need for re-addressing their existing data subnets, or adding additional ethernet ports to their switches. Leveraging the 802.1Q standard, a device such as the endpoint can tag its Ethernet frames with the VLAN ID that its traffic belongs to, placing its traffic into the voice/video VLAN (known as the auxiliary VLAN); while Ethernet frames sent by a PC are not tagged, and therefore end up in the data VLAN (known as the native VLAN). This allows the endpoint to be inserted in between an existing PC and the Ethernet switch to which it is attached, allowing for a single Ethernet port per user, thereby eliminating the need to add additional ports in the wiring closet, and allowing the endpoint to be assigned to a different (new) IP subnet rather than consuming IP addresses in the existing PC VLAN. VLANs also allow the network administrator to apply different security and Quality of Service (QoS) policies on a per-VLAN basis.

Figures 1 and 2 illustrate these concepts.

Without CDP (or LLDP-MED), the user must manually configure each endpoint with the 802.1Q VLAN ID it should use. CDP automates this task, allowing the Ethernet switch to advertise to the endpoint the ID of the VLAN it should belong to.

Automatic Quality of Service

Quality of Service is essential for a well-performing network, providing preferential service to latency, jitter or loss sensitive applications like voice and video; deferential service to misbehaving applications such as viruses and other undesirable network traffic; and fair treatment to routine, non-time sensitive traffic such as email or web browsing. However, QoS can be complex to configure and manage, and the administrator needs to be assured that the traffic entering the network is marked with the correct QoS values. For user-facing devices such as PCs, IP-based telephones and video terminals, the administrator must establish a demarcation point where QoS markings coming in from these devices are either not trusted–and instead overwritten to an administratively configured value–or trusted to set their own QoS values and the Ethernet switch will

honor those values. This demarcation point, or trust boundary, ensures that if the user accidently, or intentionally, tampers with the QoS values assigned to these devices, those QoS values will be remarked by the administrator as they ingress the network.

CDP provides a method of automatically extending this trust boundary (at the administrators' discretion) so that the phone or video terminal can mark its packets with the desired QoS values, and the switch will trust the phones packets (because the administrator knows that the specific model of phone in question can be trusted to behave properly and cannot be tampered with) and forwards those packets on into the network. This functionality is known as AutoQoS on the Cisco Catalyst line of Ethernet switches. Figures 3 and 4 illustrate the concept of AutoQoS. More information on AutoQoS can be found at

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSCampus_40.html#wp1098057

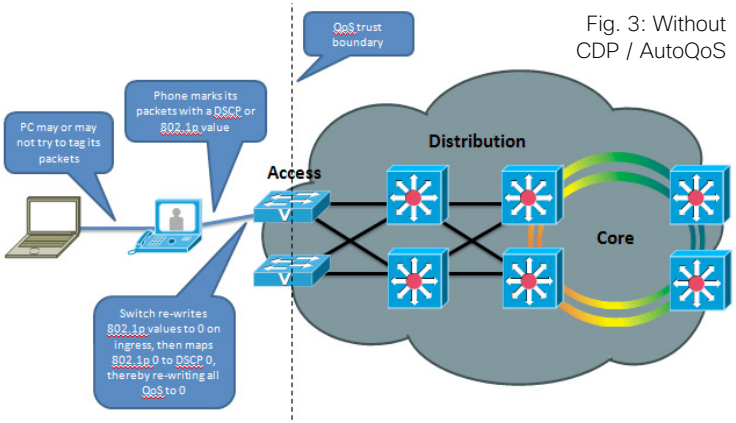


Fig. 3: Without CDP / AutoQoS

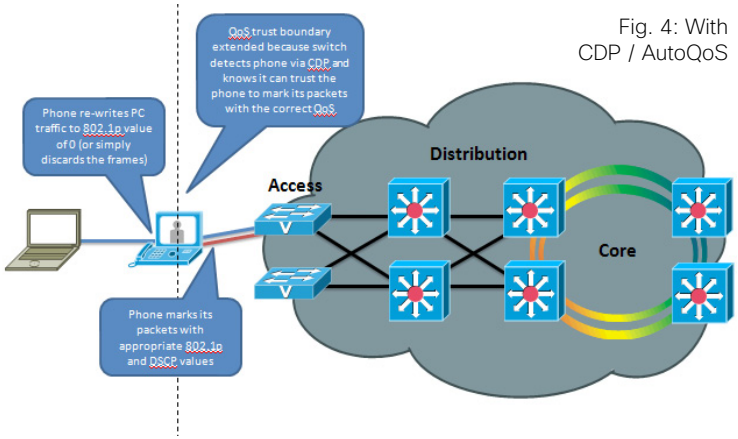


Fig. 4: With CDP / AutoQoS

Power over Ethernet (POE) negotiation

The 802.3af standard provides for Power over Ethernet to devices such as IP-based telephones and video terminals. CDP provides additional benefit by allowing the endpoint to indicate to the Ethernet switch how much power it requires–and for the switch to advertise to the endpoint how much power is available–thereby allowing more granular level of negotiation between the switch and the endpoint, and allowing the Ethernet switch to more closely track its available power budget. Note that POE is currently not used by the Cisco TelePresence endpoints, but is mentioned here as informational benefit to the reader since POE is widely used by many other models of Cisco Unified IP Phones, Wireless Access Points, surveillance cameras, and myriad other devices.

Location Awareness

With the introduction of IP-based telephones, a new level of mobility was afforded in that an IP endpoints could be plugged in anywhere in the network, obtain an IP address, and start making calls, reducing the costs associated with physically patching telephone cables when moving an employee from one office to another. However, certain management functions and emergency services rely on knowing the precise location of a telephone. CDP allows for network management applications to identify the physical location of a phone (by detecting what Ethernet port that phone is attached to, and hence, where it physically is located). This information is then leveraged by applications such as Cisco Emergency Responder to direct telephone calls made to emergency services personnel to the correct dispatch office. There are many other real and potential uses for location information.

Ethernet Speed / Duplex Mismatch Detection

Ethernet devices use the 802.3 auto negotiation procedure to automatically negotiate their speed and duplex settings. However, a very common problem is that one side or the other is accidently configured for the wrong settings, resulting in packet loss. For example, the network administrator has configured all the Gigabit Ethernet ports on the switch for auto negotiation, but the user accidently sets the port on his or her PC, IP phone or video terminal to a manually configured value, such as 100 Mbps / Full duplex. This can result in a mismatch between the switch and the endpoint, resulting in a large percentage of loss on that interface. CDP does not automate the resolution of such a condition, but it does detect it and cause an alarm to be generated on the switch, notifying the administrator of the condition so that he or she may take steps to resolve it.

Future Medianet Applications

The above benefits of CDP have been available for years from Cisco. Medianet is a new concept aimed at further extending and automating the interactions between endpoints and the network in order to deliver additional end-to-end optimization of multimedia traffic across an intelligent internetwork. CDP is one protocol, among others, that will be leveraged by future generations of Cisco IOS Software and Cisco Medianet-ready endpoints to deliver on this vision. Available Medianet applications at the time this document was written include end-to-end tracing of the path a video session takes through a network in order to pinpoint the source of packet loss, optimizing the routing of video packets over alternate paths in order to maximize the throughput of the network, enhanced Session Admission Control in order to control the amount of video sessions admitted onto the network, and more. Futher information about Medianet can be found at

http://www.cisco.com/en/US/netsol/ns1094/index.html

More information about CDP and LLDP-MED can be found at the following references

http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_cdp_discover_ps6350_TSD_Products_Configuration_Guide_Chapter.html

http://www.cisco.com/en/US/products/hw/switches/ps663/products_tech_note09186a0080094713.shtml#cdp

http://www.cisco.com/en/US/technologies/tk652/tk701/technologies_white_paper0900aecd804cd46d.html

CDP Behavior in Release TC5.0

When the Cisco TelePresence MX series, EX Series, C-Series, Profile Series and Quick Set Series endpoints running release TC5.0 are booted for the first time, or after a factory reset has been done, the following settings are applied by default:

xConfiguration Provisioning Mode: Auto

xConfiguration Network 1 VLAN Voice Mode: Off

The endpoint then displays the Provisioning Wizard screen to prompt the user for what provisioning mode they would like to use: VCS, Callway or CUCM.

If CUCM is selected by the user, then xConfiguration Provisioning Mode is automatically set to CUCM and xConfiguration Network 1 VLAN Voice Mode is automatically changed to Auto, and the endpoint begins utilizing CDP to automatically discover its VLAN and begins tagging its packets with the appropriate VLAN ID. The endpoint also begins including DHCP Option 150 in its DHCP requests so that it can automatically discover the address of the UC Manager TFTP server.

If the xConfiguration Provisioning Mode is set to VCS or Callway, then xConfiguration Network 1 VLAN Voice Mode is left in its default state of Off, and the endpoint will ignore any CDP VLAN advertisements and not tag its packets with any VLAN ID. The endpoint also does not include DHCP Option 150 in its DHCP requests.

For TMS/VCS customers, this behavior preserves the functionality they had in previous software releases of these endpoints. If CDP is desired, then it may be manually enabled by setting the xConfiguration Network 1 VLAN Voice Mode parameter to Auto. This may be done through the Touch user interface -> Administrator Settings -> Network Settings -> Link Settings, or through the On-Screen Display Menu -> Settings -> Administrator Settings -> Advanced Configuration -> Network 1 -> VLAN Voice Mode, or through the Administration web page UI -> Configuration -> Advanced Configuration -> Network 1 -> VLAN Voice Mode, or via xConfiguration Network 1 VLAN Voice Mode API/CLI command.

For CUCM customers, this behavior does present an extra step in the first-time bootup process, but once CUCM mode has been chosen in the Startup Wizard, CDP will automatically kick in and the phone will join the auxiliary (voice/video) VLAN. If the customer desires the endpoint to not use CDP, then it may be manually disabled by setting the xConfiguration Network 1 VLAN Voice Mode parameter to Off.

For customers who do not have a CDP-capable Ethernet switch, but desire to use 802.1Q VLANs, the xConfiguration Network 1 VLAN Voice Mode parameter may be set to Manual, and the associated xConfiguration Network 1 VLAN Voice ID parameter may be set to the appropriate value.

Once these parameters are set, the settings are saved and are persistent through subsequent reboots. If a user later wishes to change them, they may do so by re-running the Startup Wizard, or by manually setting the parameters individually.

Upgrades to TC5.0 from a Previous Release

For existing customers upgrading to release TC5.0 from a previous release, the existing values for these parameters will be maintained, the Startup Wizard will not be displayed, and no change in behavior will be seen by the user. Note however that the value of the xConfiguration Network 1 VLAN Voice Mode parameter have changed. In previous releases, the valid values for this parameter were Untagged or Tagged, with Untagged being the default. In release TC5.0, with the introduction of CDP support, the valid values for those parameters are now [Auto|Manual|Off]. During an upgrade, the previous values are automatically mapped to the new equivalent values.

NOTE: Management applications will need to be updated to use the new values (e.g. Off instead of Untagged, Manual instead of Tagged, or Auto) in xConfig API requests.

Table 1 below illustrates the relationship between the old and new values.

Note: The DHCP process is actually done in the background prior to the Startup Wizard being displayed. This means that during the first-time bootup, or after a factory reset has been done, the endpoint will initially obtain a DHCP lease in the native VLAN. If VLAN Voice Mode Auto is then chosen, and CDP indicates that a VLAN should be used, the endpoint will release the address it received in the native VLAN, restart its IP stack, and re-DHCP a new address in the auxiliary VLAN. This may result in temporary usage of IP addresses in the native VLAN during the first-time bootup.

Summary

This document has briefly introduced the history and benefits of the Cisco Discovery Protocol (CDP) and its behavior on the Cisco TelePresence MX series, EX series, Codec C Series, Profile series and Quick Set C20 release TC5.0. CDP is a powerful mechanism for automating the application of VLANs and Quality of Service for voice/video devices, and existing TANDBERG customers are encouraged to begin exploring its benefits and preparing their networks so that they can begin leveraging VLANs, AutoQoS and VLAN-based security policies for the former-TANDBERG endpoints.

Prior Releases	*Release TC5.0*	*Comments*
	Auto	Auto mode is introduced in release TC5.0
Tagged	Manual	Manual is the same as Tagged in prior releases
Untagged	Off	Off is the same as Untagged in prior release

Table 1: Old and New VLAN Tagging Values

User documentation on the Cisco web site

The user documentation can be found on
http://www.cisco.com/go/telepresence/docs.

Depending on which product you have, select the following in the right pane:

Cisco IP Video Phone E20:

TelePresence
> TelePresence Endpoints - Personal
> TelePresence VOIP Extensions

EX Series:

TelePresence
> TelePresence Endpoints - Personal
> TelePresence Desktop
> Cisco TelePresence System EX Series

Codec C Series:

TelePresence
> TelePresence Solutions Platform
> TelePresence Integrator Products
> Cisco TelePresence System Integrator C Series

Document categories

For each product you will find the documents under the following categories:

User guides:
Maintain and Operate > End-User Guides

Quick reference guides:
Maintain and Operate > End-User Guides

Installation guides:
Install and Upgrade > Install and Upgrade Guides

Getting started guide:
Install and Upgrade > Install and Upgrade Guides

Administrator guides:
Maintain and Operate > Maintain and Operate Guides

API reference guides:
Reference Guides > Command references

Physical interface guides:
Maintain and Operate > End-User Guides

Regulatory compliance and safety information:
Install and Upgrade > Install and Upgrade Guides

TC software release notes:
Release and General Information > Release Notes

TC software licensing information:
Release and General Information > Licensing Information

Video conferencing room guidelines:
Design > Design Guides

NOTE: All products do not have all types of user documentation.

Intellectual property rights