Exam 640-460 IIUC

CCNA Voice

Mega Guide

Prepare With Confidence

This PrepLogic Mega Guide was written by certified subject matter experts and published authors to provide you accurate, in-depth exam coverage. All exam objectives are covered in detail, giving you the knowledge and confidence you need to pass your exam.

PrepLogic

Be Prepared. Be Confident. Get Certified.

PrepLogic, Inc. • 1300 N. Westshore Boulevard, Suite # 125 • Tampa, Florida 33607
Phone: (813) 769-0920 (800) 418-6789 • Fax: (813) 769-0926 • Website: www.preplogic.com

CCNA Voice (640-460 IIUC) Mega Guide

Copyright © 2010 by PrepLogic, LLC.
Product ID: 012340
Production Date: February 23, 2010

Warning and Disclaimer

Every effort has been made to make this document as complete and as accurate as possible, but no warranty or fitness is implied. The publisher and authors assume no responsibility for errors or omissions. The information provided is on an "as is" basis. The authors and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this document.

Volume, Corporate, and Educational Sales

PrepLogic offers favorable discounts on all products when ordered in quantity. For more information, please contact PrepLogic directly:

1-800-418-6789
solutions@preplogic.com

International Contact Information

International: +1 (813) 769-0920

Australia: (02) 8003 3878

South Africa: (0) 11 083 9973

United Kingdom: (0) 20 8816 8036

Domain 1 – Components of the Cisco Unified Communications Architecture

Unified Communications (UC) Environment

Cisco has introduced what they call the Unified Communications Environment which is used to separate out the different duties of the components used with a unified communications environment.
The different layers defined in this environment include:

- **Infrastructure** – includes the routers, switches, firewalls and other devices used when transporting voice traffic.
- **Applications** – includes the applications used to provide voice services including voice mail, conferencing abilities, call center applications and 911 services.
- **Call Processing** – includes all of the devices which are used when processing a call; this includes the call setup and teardown, conferencing, and the transferring of calls among many others.
- **Endpoints** – includes the devices which are used by the end users, typically this is a phone of some sort whether physical or softphone.

UC Infrastructure Layer

The UC infrastructure layer includes all of the devices which transport the voice traffic over the network. This includes a number of devices including:

- **Routers** – used to properly route network traffic from one location inside a network to another, this is done through the use of various routing protocols. Routers also have the ability to classify, mark and process QoS information so that voice traffic is given priority over lower priority traffic.
- **Switches** – two different types can be used on a UC network, voice and data. A voice switch is used to process a call and switch it to its proper destination. A data switch or physical switch is used to connect end user equipment to the network and can both process data and voice traffic. Both types of switches have the ability to classify, mark and process QoS information.
- **Firewalls** – used to secure a network from intrusions into the network. It is possible at different points in a network that voice traffic may have to pass through a firewall device. These devices must be configured to recognize and accurately prioritize voice traffic so that it gets to the destination in a timely manner.
- **Gateways** – used between two different types of networks to translate between them. Typically a gateway is used at a point in the network where voice lines are translated into VoIP traffic and vice versa.
- **Gatekeepers** – used as a central controlling service over a number of different devices. Typically it has a picture of the whole network and helps in various duties including call routing.

UC Applications Layer

There are a number of different applications which are used to provide a variety of voice services. These applications include:

- Voice mail (Unity)
- Interactive Voice Response (IVR)
- Unified Contact Manager.
- Emergency Responder

Cisco Voicemail

Cisco's voicemail solution is called Unity and is offered in three different variants:

- Cisco Unity Express
- Cisco Unity Connection
- Cisco Unity

Cisco Unity Express

Unity express is the smallest voice mail solution provided by Cisco and is run on a supported router platform. This is possible through the use of an additional supported Advanced Integration Module (AIM) or Network Module (NM). As of this writing there are a number of different supported modules which support a number of different capabilities, these include:

- **NM-CUE** – 8-port module which supports up to 100 voice mailboxes and 100 hours of voice recordings.
- **NM-CUE-EC** – 16-port module which supports up to 250 voice mailboxes and 300 hours of voice recordings.
- **NME-CUE** – 24-port module which supports up to 250 voice mailboxes and 300 hours of voice recordings.
- **AIM-CUE** – 6-port module which supports 50 mailboxes and 14 hours of voice recordings.
- **AIM2-CUE** - 6-port module which supports 50 mailboxes and 14 hours of voice recordings.
- **ISM-SRE-300** – 10-port module which supports 100 mailboxes and 60 hours of voice recordings.

Cisco Unity Connection

Unity Connection is in the middle of the Unity solutions. It is run on a separate Linux server platform and supports many of the features that are supported in the full Unity solution but is limited by its support for 7,500 to 10,000 mailboxes. If an organization has less than 500 users Unity Connection can also be used with Cisco Unified Communications Manager on a single server. Unity Connection is also limited in the total number of ports supported. On a single server Unity connection supports up to 144 total ports when using Voicemail and 72 when using Integrated Messaging (IM). On a cluster pair 288 total ports are supported when using Voicemail and 144 when using Integrated Messaging.

Cisco Unity

Unity is the full version of Cisco's Unity voicemail product and adds all of the features which are included in both Cisco Unity Express and Cisco Connection and adds several additional features. These features include:

- Integration with legacy voicemail systems
- Connectivity with Microsoft, Lotus and Novell's email systems
- Support for up to 200 ports/sessions per server
- Support for up to 15,000 mailboxes per server
- Support for up to 250,000 total users (Across multiple servers)

Interactive Voice Response (IVR)/Auto Attendant

An important part of most modern business phone systems is an IVR and/or Auto Attendant which is used to route people to the correct people inside a company without the need for an additional person routing these calls. All of the Cisco Unity solutions provide some support for an IVR/Auto Attendant. Cisco Unity Express is limited to only 5 total levels of Auto Attendant while the others support unlimited levels. The specific features supported by each solution are listed at the link above.

Cisco Unified Contact Center

In addition to the IVR/Auto Attendant capabilities of Unity; Cisco has also developed a solution which allows call centers which receive a number of different call types to distribute the calls to the correct location inside the company and provide an easy support platform so that the operator can most efficiently resolve the purpose of the call. This is provided by the Unified Contact Center solution. Unified Contact Center is run on a dedicated server platform and allows the integration of IVR functionality with a system providing support information which can be used by the operator, this could potentially include past support ticket information or customer history information among other things. Unified Contact Center also supports chat, web and email integration abilities.

UC Call Processing Layer

The UC Call Processing Layer includes all devices which are used to process calls and provides the ability to use a number of different call features. There are a couple of main products which are used in call processing these include:

- Smart Business Communications System (SBCS) - Unified Communications 500 devices
- Unified Communications Manager Express (CME)
- Unified Communications Manager – Business Edition
- Unified Communications Manager (Call Manager)

Cisco Unified Communications 500 (UC500)

The UC500 product line was created as a single box voice/voicemail/auto attendant solution.
The UC500 products support up to 64 total users and provide all of the functionality that is needed in a small business office.

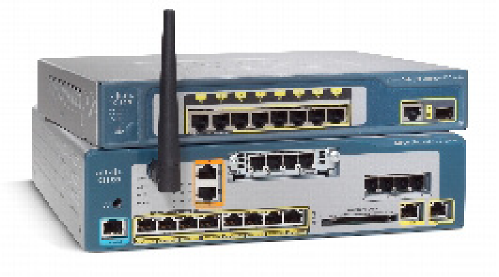


Figure 1: Unified Communications 520

Cisco Unified Communications Manager Express

Cisco's Unified Communications Manager Express solution is used in conjunction with supported routing equipment as an additional feature. There are a number of different routers which are supported. The following is a table of the supported routers when using Unified Communications Manager Express version 7.1:

Router Platform	Maximum number of phones supported
Cisco 1861 Integrated Services Router	15
Cisco IAD2430 Integrated Access Device	25
Cisco 2801 Integrated Services Router	25
Cisco 3250 Rugged Integrated Services Router	20
Cisco 3270 Rugged Integrated Services Router	48
Cisco 2811 Integrated Services Router	35
Cisco 2821 Integrated Services Router	50
Cisco 2851 Integrated Services Router	100
Cisco 3825 Integrated Services Router	175
Cisco 3845 Integrated Services Router	250
Cisco 2901 Integrated Services Router	35
Cisco 2911 Integrated Services Router	50
Cisco 2921 Integrated Services Router	100
Cisco 2951 Integrated Services Router	150
Cisco 3925 Integrated Services Router	250
Cisco 3945 Integrated Services Router	350

Table 1: Unified Cisco Manager Express 7.1 Supported Routers

Cisco Unified Communications Manager – Business Edition

The Business Edition of Cisco's Unified Communications Manager has all of the capabilities of Unified Communications Manager and Unity Connection but is limited to 500 total users and 20 total sites. Business edition differs from the Express edition in that it requires a dedicated appliance platform which is essentially a Linux server used to run the services. Version 7.1 of the Unified Communications Manager – Business Edition uses the MCS 7828 Unified Communications appliance. Business edition also has support for Cisco Unified Mobility which allows users the flexibility to route their business phones to different remote locations and to make calls remotely as if they are calling from their local phone.

Cisco Unified Communications Manager

Cisco's Unified Communications Manager which was previously called Call Manager is the full version of their call processing solution. It provides all of the features of the other versions but supports a significantly larger number of total users. Unified Communications Manager has support for over 100 sites or clusters with support for up to eight servers per cluster. Each server supports up to 7,500 Cisco Unified IP Phones or 30,000 per cluster.

Unified Communications Manager is typically run on one of Cisco's server appliances. Version 7.1 supports the MCS 7816, MCS 7825, MCS 7828, MCS 7835, and MCS 7845 devices as well as support for some IBM and HP third party servers.

UC Endpoints Layer

There are a number of different endpoints which can be used with the Unified Communications Manager devices. These include a number of different categories of devices including:

- Unified IP Phones
- SPA 500 Series IP Phones
- Software Based Phones
- Video Endpoints
- Wireless IP Phones
- Conference Stations
- Analog Telephone Adapters
- Analog Interface Network Modules
- Analog Gateway Devices

Unified IP Phones

The Unified IP phone line includes a number of different phones which have a variety of different feature sets. These phones can be used with almost any Cisco VoIP solution. There are four main classes of Unified IP phone:

Basic

The basic line of Unified IP phones is intended to be used by low volume users with a limited number of features. The following are some of the phones commonly used from the basic group of phones:

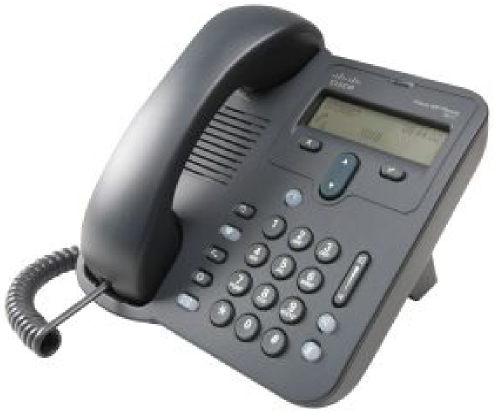


Figure 2: Unified SIP 3911

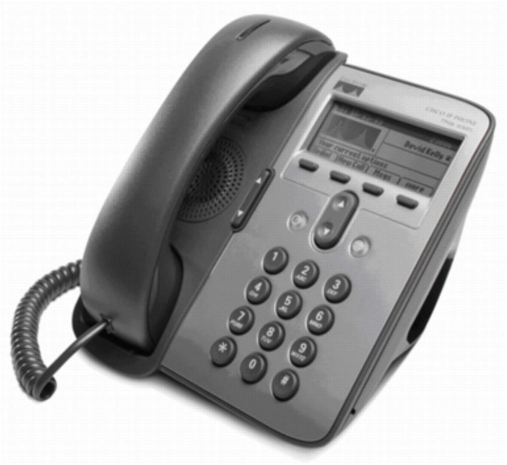


Figure 3: Unified IP Phone 7906G

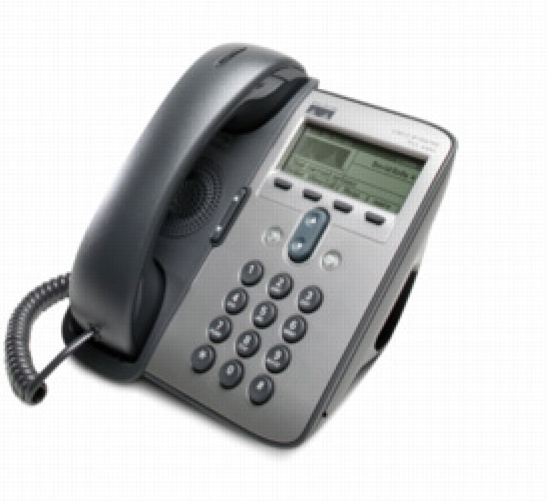


Figure 4: Unified IP Phone 7911G

Business

The business line of Unified IP phones is intended to be used by medium volume users with a large number of features. The following are some of the phones commonly used from the business group of phones:

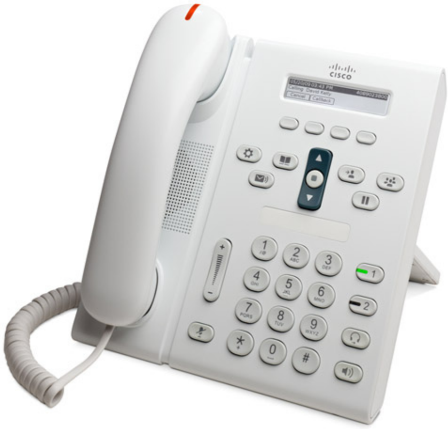


Figure 5: Unified IP Phone 6921

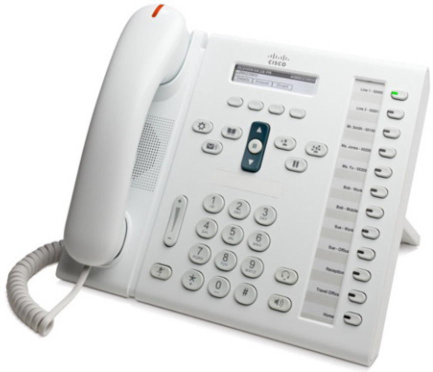


Figure 6: Unified IP Phone 6961

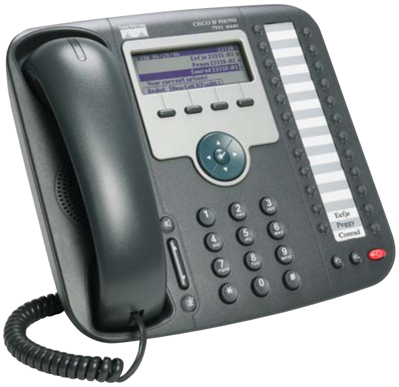


Figure 7: Unified IP Phone 7931G

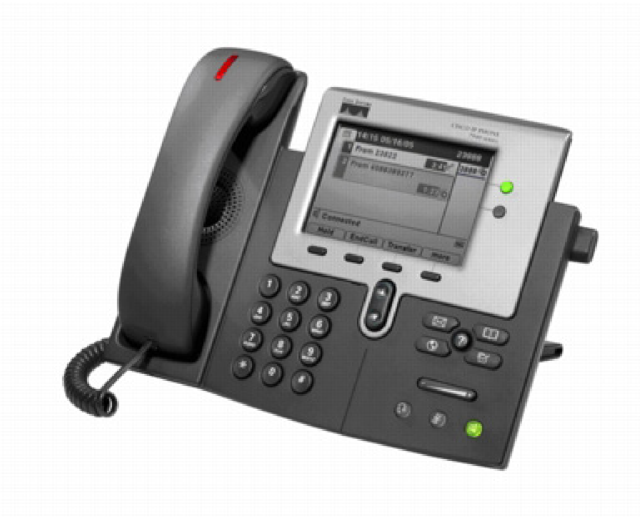


Figure 8: Unified IP Phone 7041G

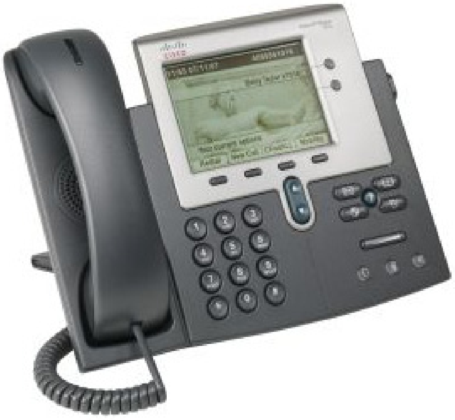


Figure 9: Unified IP Phone 7942G

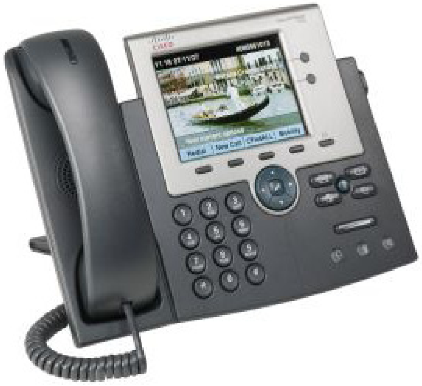


Figure 10: Unified IP Phone 7945G

Manager

The manager line of Unified IP phones is intended to be used by medium to heavy volume users with a large number of features. The following are some of the phones commonly used from the manager group of phones:

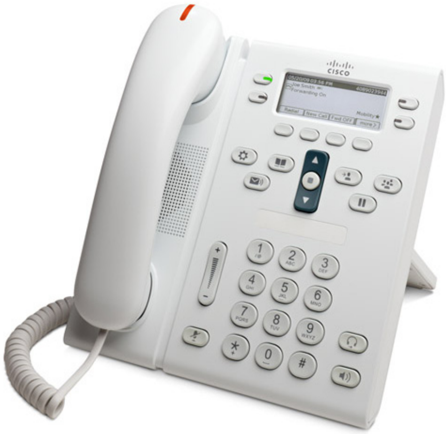


Figure 11: Unified IP Phone 6941

Executive

The executive line of Unified IP phones is intended to be used by heavy volume users with a large number of features. The following are one of the phones commonly used from the executive group of phones:

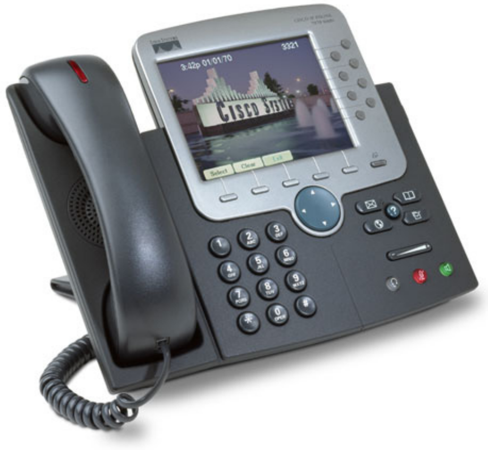


Figure 12: Unified IP Phone 7970G

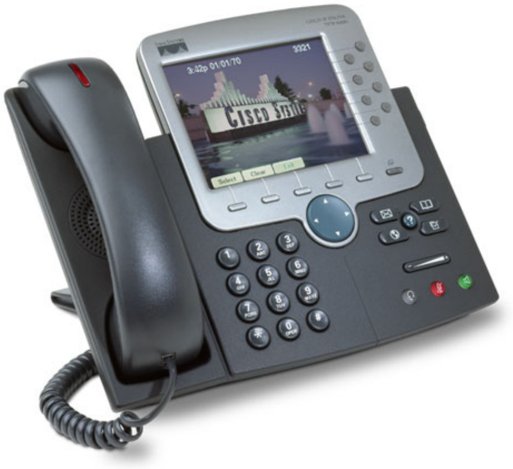


Figure 13: Unified IP Phone 7975G

SPA Series IP Phones

The SPA Series of IP phones are used strictly with the UC500 solution and provide a number of basic features. The following are one of the phones commonly used from the SPA Series line of phones:

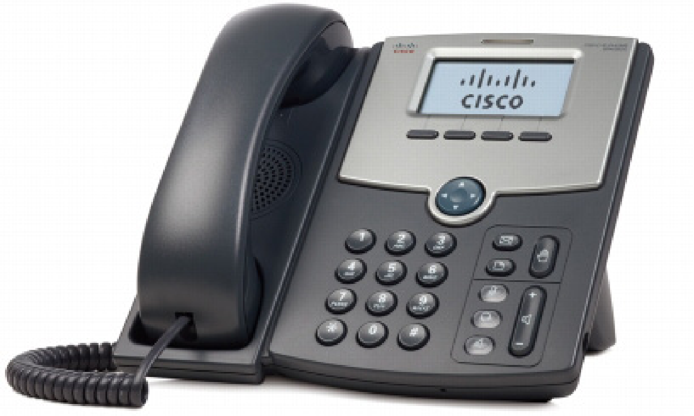


Figure 14: SPA Series 502G

Software Based Phones

A software based phone is one which is installed on a client PC and is controlled by the Unified Communications Manager. Some examples of the available options include Unified Personal Communicator and the IP Communicator.

Video Endpoints

The video line of Unified IP phones is used to provide not only voice capabilities but also video capabilities. The following is one of the phones commonly used from the video line of phones:

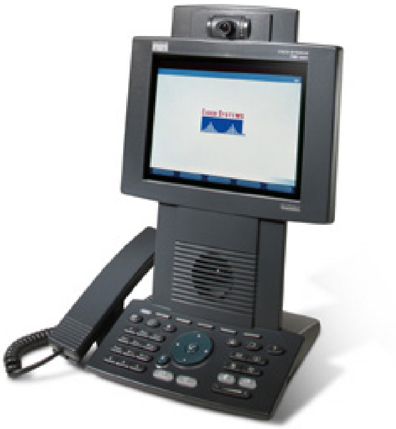


Figure 15: Unified IP Phone 7985G

Wireless IP Phones

The wireless line of Unified IP phones is used to provide voice capabilities when using a wireless network connection. The following are some of the phones commonly used from the wireless line of phones:

Figure 16: Unified Wireless IP Phone 7921G

Figure 17: Unified Wireless IP Phone 7925G

Conference Stations

The conference stations are used in an environment where voice conferences are commonly used to communicate. The following are some of the conference stations commonly used:

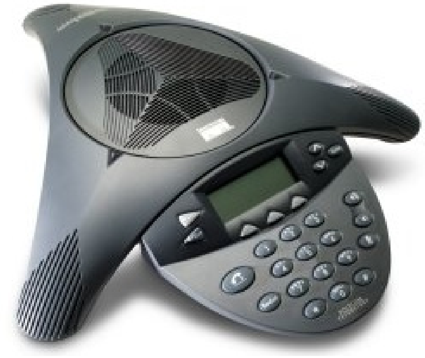


Figure 18: Conference Station 7936

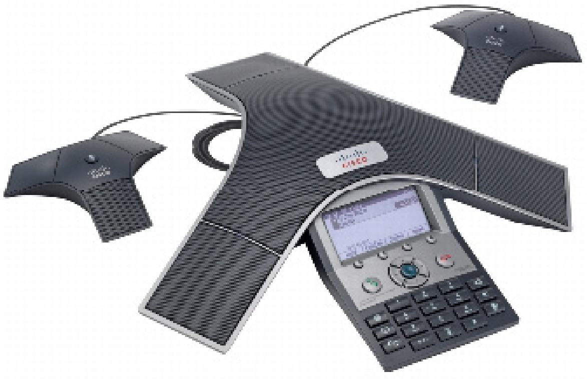


Figure 19: Conference Station 7937G

Analog Telephone Adapters (ATA)

The Cisco telephone adapters are used when a couple of analog lines are needed close to a network connection. Typically these are used for remote analog phone installations where a couple of analog lines are required. The following is one of the telephone adapter devices commonly used:

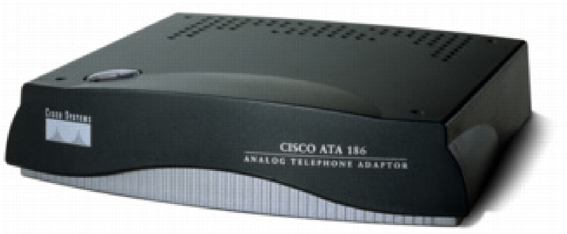


Figure 20: ATA 186 Telephone Adapter

Analog Interface Network Modules

Another endpoint device which can be used by the Unified Communications Manager is through various analog interfaces on supported routers. These routers have specific network module (NM) and Advanced Integration Modules (AIM) which provide a number of different analog port configurations.

Analog Gateway Devices

The analog gateway devices represent a way to locate a number of analog ports at a remote location where these devices are required. The smaller VG 202 and 204 devices are used with 2 and 4 ports respectively and can be used for services like fax. The VG 224 and 248 are used when a number of analog devices are located in a small area with 24 and 48 ports respectively. The following is one of the analog gateway devices commonly used:

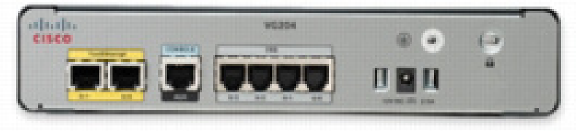


Figure 21: VG204 Analog Voice Gateway

Domain 2 – PSTN Components and Technologies

Services Provided by the PSTN

At its most basic, the Public Switched Telephone Network (PSTN) is used to complete voice calls between a calling party and a called party. Of course, in modern telephony this has been expanded to a number of different services including conference capabilities, voice mail, texting, chatting, etc. Some of which is done over the PSTN and some that are used in conjunction with the PSTN. The PSTN can also be used to achieve a data connection from one party to another as witnessed by our older viewers out there. Before the widespread use of broadband technologies most typical home users were limited to using a modem in conjunction with the PSTN to connect to a remote information connection point.

Time Division and Statistical Multiplexing

Time Division Multiplexing

Time Division Multiplexing (TDM) is used on many circuit types including T1 and E1s. TDM works by allotting specific channels to specific data and 'weaving' each of these channels into one another. With a T1 there can be 24 separate data streams which all seem to be sent at the same time but are really sent one after the other in order and repeated. Because these types of circuits rely so much on specific timeslots the synchronization of the connecting networks must be of high priority.

Statistical Multiplexing

Statistical Multiplexing is different from TDM as it does not allot specific timeslots for different data streams. What happens with statistical multiplexing is that multiple streams of data are able to be transferred at the same time and are multiplexed together depending on the required bandwidth of the stream. Some examples of Statistical multiplexing technologies are TCP/IP and UDP/IP. Statistical Multiplexing is considered to be more efficient that TDM because the timeslots are only allocated when needed as opposed to TDM where the timeslots are allocated even if they are not used.

Analog Circuits

Inside voice networks there are three different types of analog circuits or interfaces:

- Foreign Exchange Office (FXO)
- Foreign Exchange Station (FXS)
- Earth and Magneto (E&M)

FXO and FXS interfaces are used with one another, the FXO interface is connected to the telephony switch and the FXS interface is connected to the telephone equipment (phone). When a call comes in, the FXO interface is alerted via ring voltage from the switch then the FXO interface tries to transport the signal to the FXS. The FXS is responsible for receiving the signal from the FXO and providing battery, dial tone and other signaling to the telephone equipment. The E&M interfaces are typically used to connect Private Branch Exchanges (PBX) which exists inside offices. The PBX is essentially a small telephony switch that allows different features to be used inside an office environment; these types of features include extensions, forwarding, and conferencing among others. Tie Lines are used when connecting together two or more different PBX's that are typically using E & M as the interface. There are five different types of E&M interfaces; types I through V (1 through 5). The details of each interface are beyond the scope of this guide but types I and V are the most common; Type I is typical in North America and Type V is typical outside North America.

Digital Voice Circuits

Within VoIP there are a couple of different digital circuits or interfaces; Basic Rate Interface (BRI), T1 and E1 being the main ones.

A BRI is used for small office connectivity and provides two channels of voice (64 kbps each), which are called B-Channels and an independent signaling channel (16-kbps), known as the D-Channel. The data link layer of the D-Channel is Q.921 and control signaling is typically done through Q.931. T1 signaling often gets confused because there are two different ways to signal with a T1 interface. The two different ways are:

- **Channel-Associated Signaling (CAS)**
    - Uses robbed-bit signaling.
    - T1s are divided into frames which fit into either a Superframe (SF – 12 Frames) or an Extended Superframe (ESF – 24 Frames).
    - Each frame includes 24 timeslots used for the 24 T1 channels and each frame includes 8 bits of each channel plus a framing bit.
    - The 6th and 12th channels have their low order bit "robbed" for use in signaling.
- **Common Channel Signaling (CCS)**
    - Uses one full 64-kbps channel for signaling and leaves the other 23 channels for traffic.
    - This configuration is typically called a Private Rate Interface (PRI).
    - BRI is still considered a CCS interface using one full 16-kbps signaling channel.

E1s all operate the same in a CCS configuration (sometimes they can be incorrectly called CAS). An E1 interface includes a total of 32 channels, with 30 being used for traffic. E1s are split similar to T1s except their framing is a little different. E1s are split into multiframes which include 16 contiguous frames and each frame includes 8-bits of each channel. The 1st and 17th channels are used for frame synchronization and signaling, accordingly. There are no framing bits within an E1 like T1s have.

An alternate to Q.931 is **Q Signaling** (QSIG) which is used as an interconnection between PBX, key systems and Cisco Call manager. QSIG consists of three sublayers: Basic Call, Generic Function and Supplementary services.

Analog Line and Trunk Signals

Before we go into the details of the various types of signaling we need to provide a list of the available signals which are sent over these lines or trunks. These include three major groups: supervisory signals, informational signals and address signals.

Supervisory Signals

- **On-Hook** – the connection is effectively down and not in the process of a call or on an active call.
- **Off-Hook** – the connection is actively trying to communicate and electrical signals are allowed to pass. This is also called seizure.
- **Ringing** – the connection is actively trying to gain the attention of the opposing side.

Information Signals

- **Dial Tone** – indicates a readiness for the receipt of digits.
- **Busy** – indicates that the remote console is in use.
- **Ringback** – indicates that the remote console is currently ringing.
- **Congestion** – indicates that the telephone long distance network is unable to complete a call.
- **Reorder** – indicates that the telephone local network is unable to complete a call.
- **Receiver off-hook** – indicates that the receiver has been off-hook for a long amount of time.
- **No such number** – indicates that the dialed number is invalid
- **Confirmation** – indicates that the telephone network is attempting to complete a call.

Addressing Signals

- **Dual-tone Multi-frequency (DTMF)** – the most common type of address signaling in the U.S. and is indicates by both a high and low tone being transmitted over the line to indicate a specific digit.
- **Pulse** – typical when using rotary dial phones and works by connecting and disconnecting the local loop in various patterns as to indicate a specific digit.

Analog Line and Trunk Signaling

There are five different types of line and trunk signaling: Loop-start, Ground-start, E&M wink-start, E&M immediate-start and E&M delay-start.

Loop-Start Signaling

Loop-start signaling is the most common in a normal home telephone. With loop-start signaling the path from the telephony Central Office (CO) and the subscriber equipment is seen as a simple loop with voltage and ground provided by the CO. When the phone is on-hook the telephone will break this loop and thus no voltage will exist across the line.

When the subscriber takes the telephone off-hook, the telephone will connect the loop and voltage will exist on the line, once this happens the CO switching equipment will see the voltage and offer a dial tone. If the phone is being called the CO will send a ringing voltage over the line, the telephone will see the differing voltage and initiate a ring. If the telephone is answered by coming off-hook then the telephone will connect the loop together, once this happens the CO switching equipment drops the ringing voltage and passes on the call. Loop-start works well for home services but is susceptible to *glare* which is what happens when both the switching equipment and the subscriber equipment try to come off-hook at the same time.

Ground-Start Signaling

Ground-start signaling works a little differently. Before we describe this much more we must review some terminology. Back in the days of phone operators, there was a type of wire connection resembling a modern day ¼" audio jack (headphone). This type of connected had two points of connection, the *tip* and the *ring***.** In modern equipment, the *tip* typically is connected to the ground and the *ring* is typically connected to the voltage side.

With ground-start, there is a requirement that both sides of the connection be separately grounded. In an idle or on-hook state the subscriber equipment has a break in the *ring* and the CO equipment has a break in the *tip*. When the subscriber side seizes the line, it grounds the *ring* side of the connection. The CO equipment sees this and, in response, grounds the *tip* side of the connection. At this point the subscriber sees the grounded *tip* and connects the loop together and removes the ground from the *ring* side. When the CO equipment wants to seize the line it grounds the *tip* side of the connection, in response the subscriber equipment closes the loop and removes the *ring* ground connection. Ground-start signaling reduces the incidence of *glare* but does require a common ground.

E&M Signaling

E&M signaling trunks are wired differently than FXS or FXO. The E&M line uses 8 wires and these wires are laid out as follows:

Lead	Description	Pin
SB	Signaling Battery	1
M	Signaling Input	2
R	Ring, Audio Input	3
R1	Ring, Audio Input/Output	4
T1	Tip, Audio Input/Output	5
T	Tip, Audio Input	6
E	Signaling, Output	7
SG	Signaling Ground	8

Table 2: E&M Leads

E&M wink-start works by utilizing a pulse or *wink* of 140 to 290 ms to signal the receiving switch as ready for digits. When the originating switch seizes the line (typically using the M lead) it signals the remote side using the signaling leads as defined by the E&M type. The remote switch sees the line seizer on the E lead and transmits a *wink* by going off-hook from 140 to 290 ms, then returning to on-hook. The originating switch detects the *wink* then waits at least 100 ms and sends output digits.

E&M immediate-start works when the originating switch seizes the line and instead of waiting for a *wink* acknowledgement it waits a predetermined amount of time (> 150 ms) and transmits output digits. The remote switch only acknowledges the originating switch when the call is answered and the M lead is raised.

E&M delay-start works when the originating switch seizes the line by raising its M lead the remote switch acknowledges by raising its M lead. Once the remote switch is ready for output digits it will lower its M lead, once this happens the originating switch will send output digits.

Domain 3 –VoIP Components and Technologies

The Process of Voice Packetization

Traffic Packetization

In order for an analog voice signal to be transmitted across a digital network, it must first be digitized. This is done through a process known as packetization. As shown in the following figure, packetization takes an analog waveform and converts it into a stream of digital 1's and 0's.

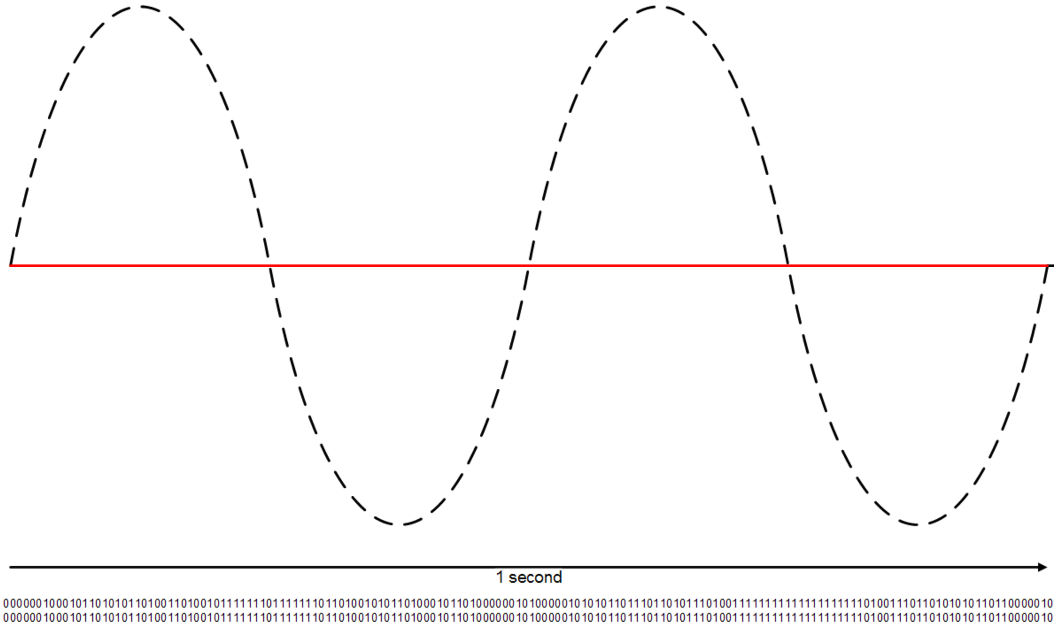


Figure 22: Packetization

Sampling

The first step in digitizing a signal is to turn the analog wave into something that can be digitized. This is done through sampling. Sampling takes slices of the analog wave at consistent intervals. The Nyquist–Shannon sampling theorem is integral to the concept of sampling.

This theorem states that, in order to adequately represent an analog signal digitally, the analog signal must be sampled at a rate twice the highest analog frequency. Within voice networks, the frequencies from 300 to 3400 Hz are transmitted; for simplicity's sake, we sample from 0 to 4000 Hz over digital lines. Following the Nyquist–Shannon theorem, this means that analog signals must be sampled at 8000 Hz—8000 samples per second. In order to demonstrate this process, we have cut the following figures down to 40 Hz.

First, the analog signal must be separated into pieces, because 40 Hz sampling is being shown, this analog signal is split into 40 different pieces (samples).

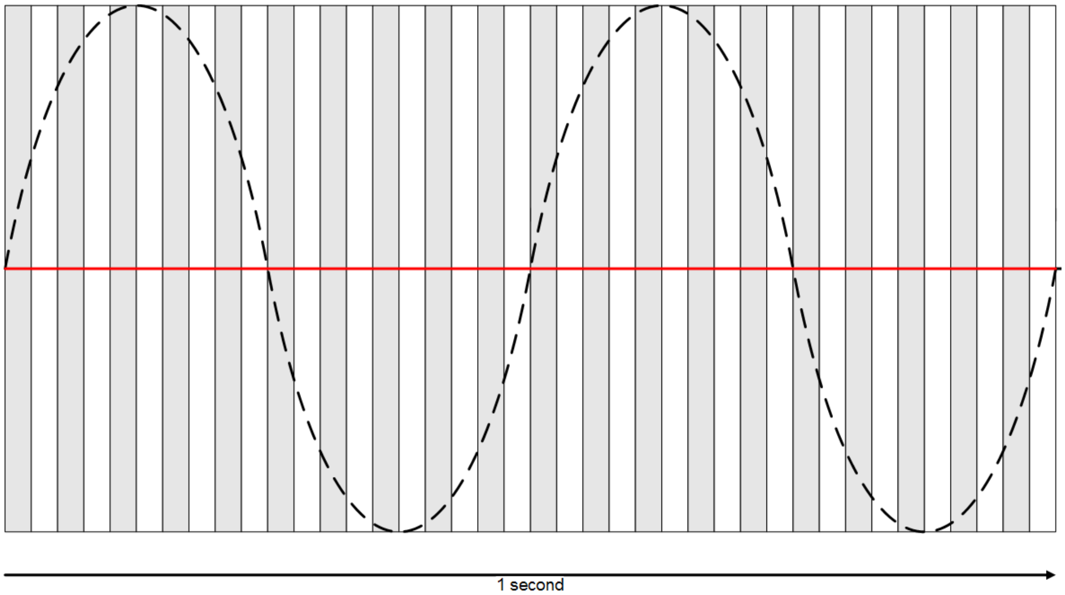


Figure 23: Separating the Analog Signal

From these, only the pieces (samples) are taken that best represent the analog signal:

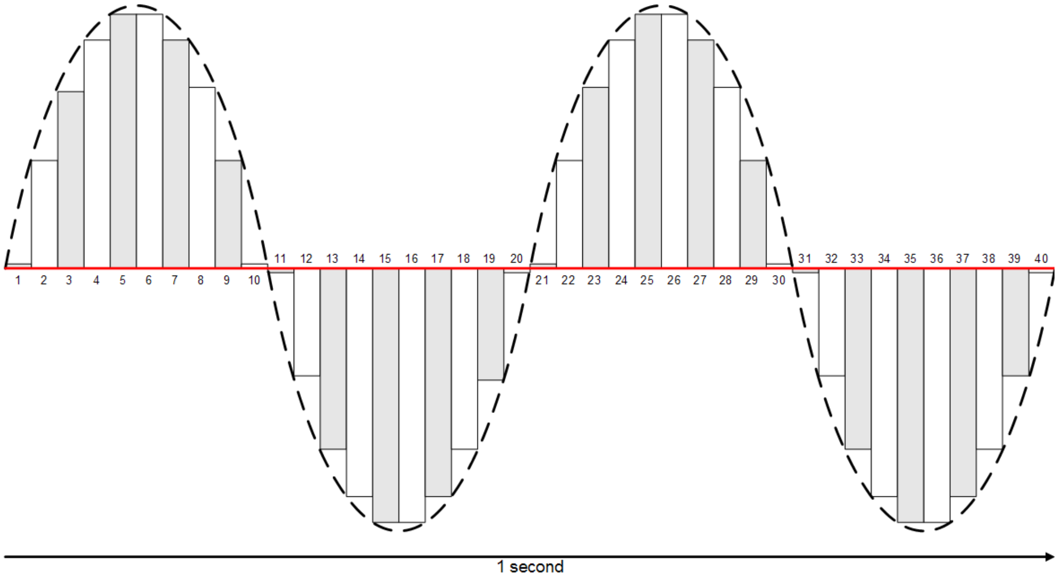


Figure 24: Creating Samples

From this figure it is seen that the digital samples represent a signal similar to the analog signal being converted. Obviously, the more samples that are taken the more likely the original analog signal the digital representation will be.

Quantization

Quantization calculates a mathematical value for each sample taken; quantization is also called companding or compansion. For the purposes of this example, we will describe Pulse Code Modulation (PCM), or G.711. With standard 64 kbps PCM, samples can be assigned a range from -127 to +127, which are from the 8 bits used to record the signal; in the following figure, each sample is given a number in the range.

When the whole signal is given uniform translation, regardless of the level of the signal, it is called uniform (or linear) quantization. Uniform quantization results in low level signals having a higher Signal-to-Noise (SNR) ratio than higher level signals. Because most signals are lower in nature, this is inefficient. The problem is remedied with two different companding algorithms, μ-law and a-law.

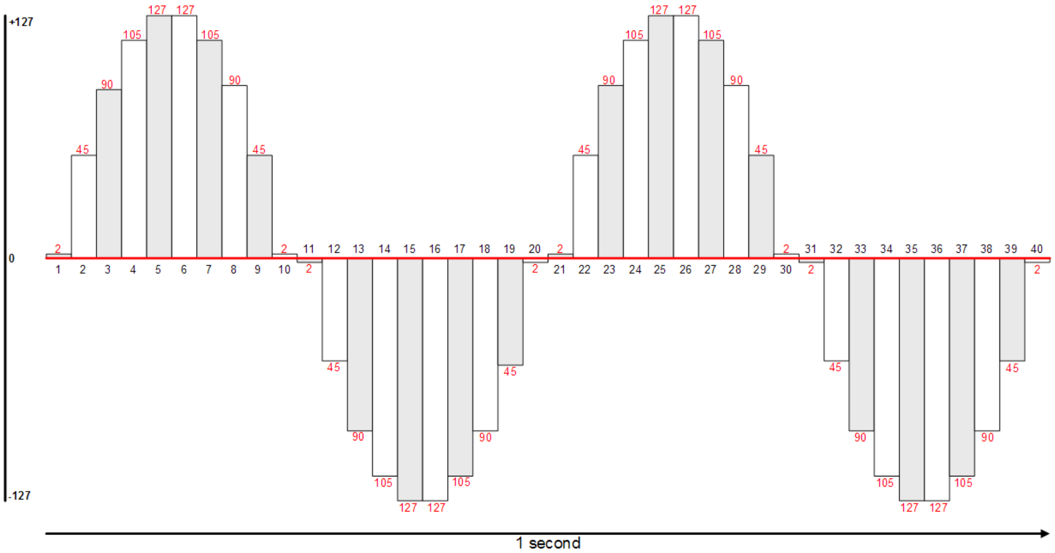


Figure 25: Quantization

μ-law (mu-law) is the formal standard in North America and in Japan; a-law is used in the rest of the international community. These two algorithms work by taking a 14-bit (μ-law) or 13-bit (a-law) PCM sample and mapping it logarithmically to an 8 bit sample. Put simpler, this means that a larger signal is compressed down (14 or 13 bit) to fit in an 8-bit space and, in order to remedy the linear quantization problem, both μ-law and a-law encode lower level signals at smaller step intervals and higher level signals at higher step intervals. Both of these algorithms effectively increase the Signal to Noise (SNR) ratio of the signal. It is also standard in μ-law countries to convert to a-law in order to communicate with a-law countries.

In order to make these numbers into a stream which can be transmitted digitally as binary, encoding is needed. With PCM, the encoding process takes each number and converts it into a 7-bit binary number with the 1st bit being used to denote the sign (or *polarity*) with 1 meaning negative and 0 meaning positive, the 2nd, 3rd, and 4th bits signifying the *segment*, and the 5th, 6th, 7th and 8th bits signifying the *step*. Once the signal is converted to binary it is run through a digital to digital conversion process which shapes the signal for transmission. The following figure shows this process:

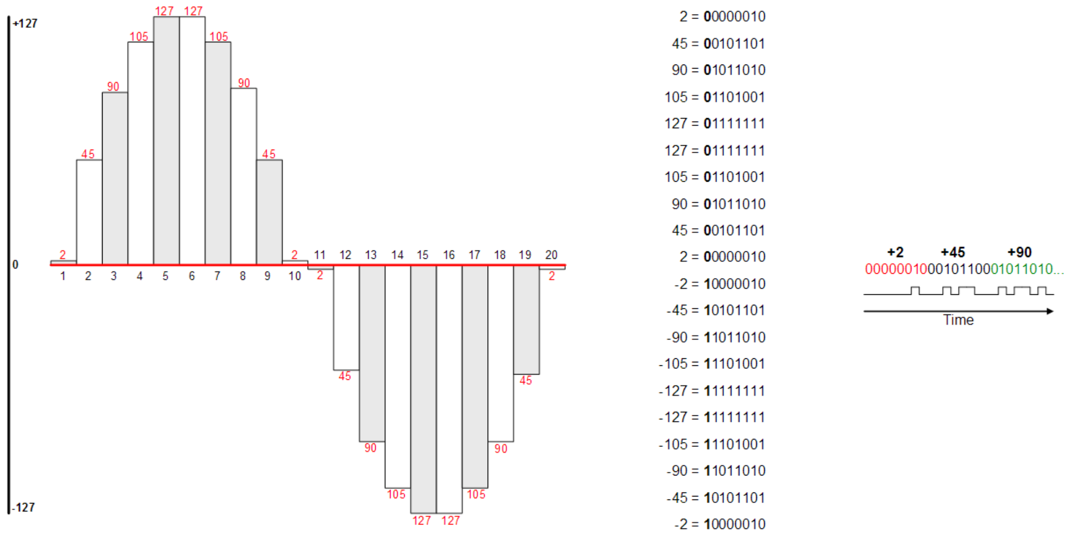


Figure 26: Binary and Digital-to-Digital Encoding

Depending on the codec which is used on the signal this quantization phase operates in different ways in order to achieve bandwidth savings.

RTP and RTCP

Real-time Transport Protocol (RTP)

All voice over traffic (not signaling) is carried via UDP; however, UDP, by itself, has some problems that need to be addressed for Voice over IP service to work. UDP by itself does not have packet sequencing and reordering capabilities or the ability to time stamp. Because of these shortfalls another protocol, Real-Time Transport Protocol (RTP) was created to run over UDP and provide these capabilities.
These capabilities on top of UDP's ability to multiplex traffic make voice over technologies work well and keep a high quality level. RTP is used with all of the VoIP protocols. The problem with RTP is that its header adds extra overhead to the voice packet, 12 bytes in total for voice with an additional 60 bytes possible if optional headers are used for other types of media streams.

RTP Control Protocol (RTCP)

RTP also has a monitoring protocol that works with it called Real-Time Transport Control Protocol (RTCP). RTCP is used to monitor the RTP session and update the participants of the status of the stream.
This functionality is typically used for Quality of Service (QoS). The devices which control the QoS on the gateways use this information to control the flow of RTP. The traffic service parameters could need to be changed or the codec might need to be changed based on available RTCP data.

Coder – Decoder (Codec)

Describe the function of and differences between codec's

Compression is the main thing that has driven the use of VoIP. Through the use of compression, many voice calls can be conducted in the same amount of bandwidth as one had in the past. There are a couple of compression standards (International Telecommunication Union – ITU); these are called codec standards. The following table lists the standard codec's that are in use today:

Codec	Acronym	Name	Bit Rate
G.711	PCM	Pulse Code Modulation	64-kbps
G.722	SB-ADPCM	Sub-Band ADPCM	48, 56, 64-kbps
G.722.1	MLT	Modulated Lapped Transform	24 and 32-kbps
G.722.2	ACELP	Algebraic Code Excited Linear Prediction Coder	6.60, 8.85, 12.65, 14.25, 15.85, 18.25, 19.85, 23.05 or 23.85-kbps
G.723.1 (5.3-kbps)	ACELP	Algebraic Code Excited Linear Prediction Coder	5.3-kbps
G.723.1 (6.3-kbps)	MP-MLQ	Multi Pulse-Maximum Likelihood Quantization	6.3-kbps
G.726	ADPCM	Adaptive Differential Pulse Code Modulation	16, 24 and 32-kbps
G.728	LDCELP	Low Delay Code Exited Linear Prediction	16-kbps
G.729	CS-ACELP	Conjugate Structure Algebraic CELP (High Complexity)	8-kbps
G.729A	CS-ACELP Annex A	Conjugate Structure Algebraic CELP Annex A (Lower Complexity then G.729) (Medium Complexity)	8-kbps
G.729B	CS-ACELP	Conjugate Structure Algebraic CELP (G.729 with silence compression support) (High Complexity)	8-kbps
G.729AB	CS-ACELP	Conjugate Structure Algebraic CELP (G.729 A with silence compression support) (Medium Complexity)	8-kbps
RFC3951	iLBC	Internet Low Bitrate Codec	13.3, 15.2-kbps

Table 3: Voice Codecs

Choosing the Appropriate Codec

The type of codec which is chosen depends on a couple of factors including the voice quality sought, the bandwidth available and delay expected between voice devices. Each of the codec's is benchmarked using a Mean Opinion Score (MOS), the MOS scale rates a codec from 1 (Bad Quality) through 5 (Great Quality). Another major factor is cost; each specific type of codec chosen uses a specific amount of Digital Signal Processing (DSP) resources.

There are three levels of complexity between codec's: low, medium and high. The following table shows some of the codec's and their complexity:

Codec Complexity	**Codec**
Low	G.711 (μ-law and a-law) Fax Pass-through
Medium	G.729A G.729AB G.726 Fax Relay
High	G.729 G.729B G.728 G.723.1 G.723.1A Modem Relay

Table 4: Codec Complexity

H.323

Components

- **H.323 Gateway –** used to translate between different types of connections. With H.323 this includes analog phones, trunks, and various other interfaces. The H.323 gateway also has the capability to place and receive calls with or without the use of a gatekeeper.
- **H.323 Gatekeeper** – acts as a central point for resolving H.323 phone numbers and IP addresses and also to control admission control. The gatekeeper also takes care of call routing and control, security and bandwidth management.
- **H.323 Terminal** – a device which can do any real-time two-way communication. These devices include IP phones, conferencing equipment, gateways and Call Managers.

H.323 Call Flow

Rather than define a specific protocol, H.323 specifies a group of protocols that are used to connect devices together through a distributed model. With H.323, this includes not only voice services but also video. There are four phases involved in creating an H.323 connection.

- **Admission Request Phase** – endpoint or gateway communicates with the gatekeeper via H.225 over UDP.
    1. The gatekeeper checks to see if it knows how to route the call requested.
    2. If the call route exists, the gatekeeper checks if a path is available between the two endpoints with available resources.
    3. If resources are available, then the gatekeeper performs an address translation from phone number to IP address and returns the information to the requesting endpoint.
    4. The admission is done through Registration, Admission and Status (RAS) messages. For admission this is done through Admission Requests (ARQ) and Admission Confirm (ARF) messages.
- **Connection Setup –** endpoints communicate directly via H.225 over TCP.
    1. During this phase, the endpoints take the lookup information and establish a connection to the endpoint.
    2. A setup message is sent from the originating endpoint.
    3. If the call is accepted a connect message is exchanged.
- **Capabilities Exchange –** endpoints communicate directly via H.245 over TCP. Capabilities which are exchanged include voice or video communications, codec exchange, compression exchange and coding exchange including others. It is at the end of this phase that the end user is finally notified of an incoming call.
- **Opening the Media** – occurs via H.225 over TCP. If the end user has answered the call connect messages are used to open the connection. Once the call is complete then the call is released using H.225, this is done through Disengage Requests (DRQ) and Disengage Confirm (DRF) messages.

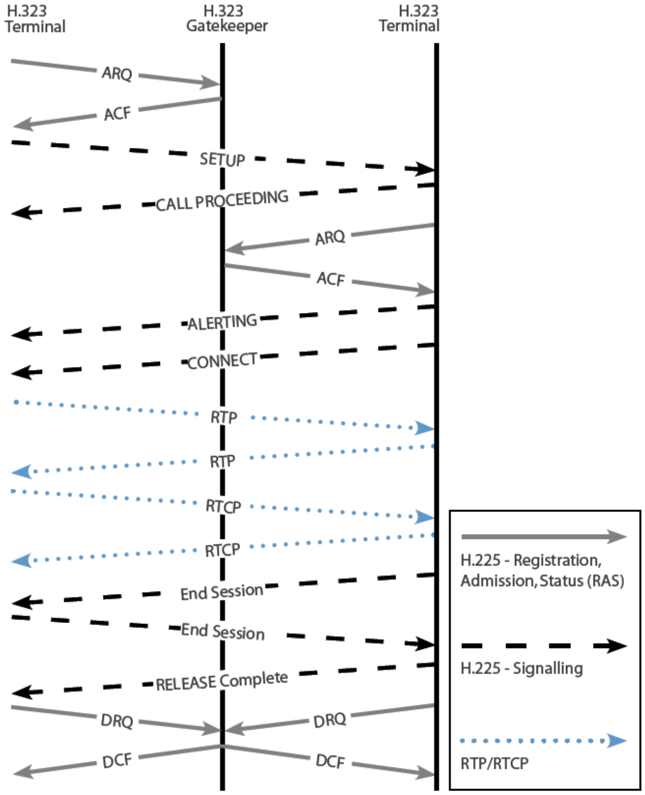


Figure 27: H.323 Call Flow

MGCP

The **Media Gateway Control Protocol** (MGCP) works a little differently than the other two protocols. MGCP works by controlling multiple gateways. Within MGCP there are two main components, the Media Gateway (MG) and the Media Gateway Controller (MGC). The MGs are responsible for connecting and translating connections into the network. These can exist anywhere from the end user's house to a central telephone office. The MGC is the call agent and is responsible for call control; for more information on Call Agents see the Central call control model section. With MGCP if the connection to the MGC is removed then the gateways do not know how to independently route calls; this functionality is completely up to the MGC.

The MGCP has two main types of gateway, a residential gateway and a trunking gateway. Residential gateways handle the interfaces like analog ports and VoIP networking interface. The trunking gateways handle the interfaces which go out to the PSTN network.

MGCP Call Flow

We must establish that the gatekeepers in the case of Cisco are Cisco Call Manager and the gateways can be various network equipment which supports MGCP voice. The following shows a call from one analog phone to another:

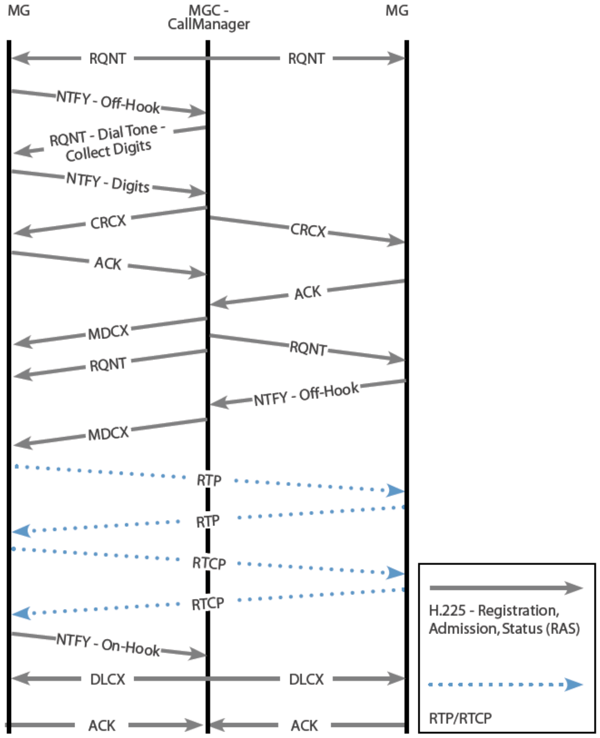


Figure 28: MGCP Call Flow

SCCP

Skinny Call Control Protocol (SCCP) is a proprietary legacy Cisco protocol which is used to connect SCCP clients to a Call Agent (Call Manager). SCCP is not typically deployed in current networks and is included in this guide as a general reference. The only devices which may be seen using this protocol in modern networks are some Cisco IP phones (7900 Series), but for the most part, one of the other protocols described in the document will be in use.

SIP

Session Initiation Protocol (SIP) is similar to H.323, in that it works as a distributed model and uses several different separate protocols. Unlike H.323, SIP was developed with the Internet in mind and, as such, is text-based similarly to the Hypertext Markup Language (HTML). SIP also is addressed similarly to web pages, with a URL:

```
sip:far-end-user@testing.com
```

As a protocol, SIP is used to initiate and find the target recipient. Once the recipient is found, the Session Announcement Protocol (SAP) takes over by identifying what type of session is trying to be established (voice or video). This is carried over the network with the Session Description Protocol (SDP). SAP and SDP are used to create or change the parameters of a call.

SIP was built to perform four basic functions: locate users and resolve their information, negotiate capabilities, change sessions during a call, and manage the setup and teardown of the call. Since SIP is Internet-minded, the Domain Name Server (DNS) can be used to lookup and resolve user's SIP information. SIP also introduces enhanced presence abilities; this enables the SIP end-points or User Agents (UA) to notify other parties as to their willingness and ability to take a call. Additionally, SIP defines Watchers who have the ability to receive information regarding the SIP presence of other subscribers. With SIP, these UAs are also separated into two entities: the User Agent Client (UAC) and the User Agent Server (UAS). The UAC is the calling party and the UAS is the called party.

SIP Components

- **Proxy Server –** has the ability to perform call routing, authentication, authorization, address resolution and loop detection. The proxy servers attempt to locate the called party and will relay the SIP messages along the path it finds in addition to updating the calling party (UA). Once a call setup is complete, the proxy server can be kept in the signaling path in order to see call change or termination messages.

  It is important to note that a proxy server is not needed with SIP for end-to-end communications.
- **Redirect Server –** has the ability to keep track of UA's which change their location either permanently or temporarily. The redirect server also has the capability to return multiple possible addresses.
- **Registrar Server –** used by the UA's to register and find location information. The registrar server takes this information and places it onto the location server. Other servers in the SIP network query the registrar server for the location of called parties.
- **Location Server –** maintains the location database.
- **Presence Server –** responsible for gathering presence information from the presentities (UAs) and subscription information for the watchers (Other UA's).

SIP Call Flow

The following SIP call flow examples show two different situations. The first example shows the traffic between SIP gateways when one analog telephone calls another. The second example shows a native SIP device calling an analog phone via a proxy server.

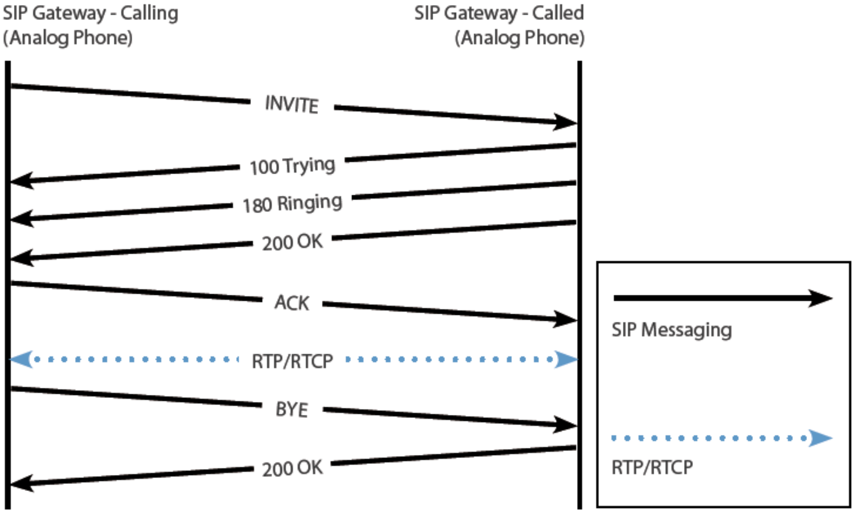


Figure 29: SIP Call Flow (Between analog phones)

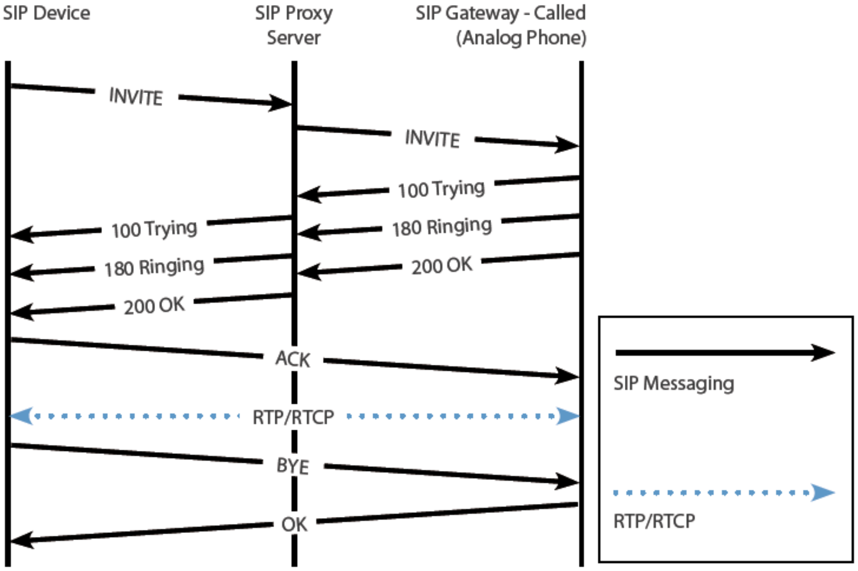


Figure 30: SIP Call Flow (Between SIP device and analog using proxy)

Domain 4 – Gateways, Voice Ports and Dial Peers

Function and Application of a Dial Plan

Numbering Plans

The easiest way to describe a numbering plan is to think about it in terms of an IP numbering plan. When building an IP network, it is very important to lay out numbering for the whole network before deployment. If this isn't done, the IP space will not be hieratical, making routing and summarization on medium or large networks very cumbersome; troubleshooting becomes almost impossible.

A number plan in the voice world is just as important. Consider the telephone number you have right now. What if everyone's phone number had a different area code and prefix? This addressing scheme, while possible, would be confusing for the end user. Now think about how this would be as the network operator, how would calls be correctly routed. Every voice routing device would have to keep a complete routing table of every number, this is because the simple summarization that happens in every Central Office (CO) would not be possible.

The International community follows a basic standard numbering scheme in order to interoperate; this is done through the E.164 standard. This standard lays out a one to three digit country code which is used by all countries to route calls to each individual country. Once this is done, each country is responsible for creating a national numbering plan; in North America this is done through North American Numbering Plan (NANP). To all who are familiar with North American number this will be familiar. The NANP follows a 10 digit numbering plan with a three digit Numbering Plan Area (NPA) which is used to identify an area, which is also why it is called the area code. A three digit code which is then used to identify a central office or exchange, this is also referred to as the NXX. And the final piece is the four digit station code which defines the specific phone or location.

Dial Plans

A dial plan differs from a numbering plan in that it defines how the numbering plan is dialed in a specific region. For example, this is why in certain regions a 7-digit number is all that is required to dial but in other areas the whole 10 or 11-digit number is required.

Function and Application of Voice Gateways and Ports

The gateway is an easy concept to understand, as it is simply a translator between one type of language or interface and another. When talking specifically about an IP voice gateway the relationship is typically from an analog trunk/port or digital trunk/port to a packet based media. This media can be anything which can support IP from an Ethernet connection to a T1 which has IP running over HDLC/PPP. A simple example of this would be from a standard Foreign Exchange Station (FXS) analog port (what would connect to a typical analog telephone) to an Internet connection (e.g., Vonage or Skype). The IP gateway is responsible for taking the traffic from the analog FXS port and encoding it and transmitting it over the Internet connection running IP and in the reverse direction decoding the traffic from the Internet connection and formatting it over the FXS port. The voice gateway also has some other duties beyond simple translation, including:

- Support for various call control protocols
- Call setup and teardown
- Call hold
- Call transfer
- DTMF relay

On Cisco equipment, the call control protocols typically used are Media Gateway Control Protocol (MGCP), H.323, and Session Initiation Protocol (SIP) as well as various other supplementary protocols. Included with the support for these call control protocols is the responsibility for encoding and decoding a variety of different codecs which are used to efficiently send this traffic over a digital medium.

Gateways on VoIP networks typically involve translating an analog line to a digital one; for example an FXS line to a telephone goes into a gateway to be translated onto a digital trunk line to the PSTN. When this happens the gateway must be able to understand not only the way to communicate with the telephone but also with the trunk line. When someone picks up the telephone, it is the responsibility of the gateway to see this off-hook status and initiate dial tone to the telephone, be able to receive digits and be able to correctly route the call on to the appropriate trunk line.

This process, of course, greatly depends on the types of interfaces being used on both the sending and receiving ends. Without the use of a gatekeeper, the gateway must be configured with a complete picture of the VoIP network so that calls which are put through the gateway can be understood and routed. If this is not true, the gateway would be just as useless as a common router without an empty routing table.

There are a number of ways to configure a gateway and a number of interfaces which are supported. With each of these interfaces are specific configured parameters that are specific to each. The following sections will go over the various common lines (or ports) which can be configured on Cisco equipment. There are also a number of different features which are common to voice networks which are also supported on this equipment. These will also be detailed in the following sections from the perspective of the gateway not using a gatekeeper.

Configuring Voice Ports

Configuring Analog Voice Ports

The configuration of analog voice ports is one of the most basic functions which are required for Cisco equipment to work in the voice world. The Cisco equipment must have a port-adapter installed that supports the type of interface that is required. The following section goes over the basic steps which are required for each different type of analog interface.

FXS and FXO

1. Enter voice-port configuration mode through the **voice-port** command.
2. Configure the access signaling type. On an FXS port, your options are loop-start and ground-start. Use **signal** *loop-start* | *ground-start*.
3. Configure call progress tones. Ring and cadence are all configured with the same command: **cptone** *locale.* The *locale* used in this command is a two-letter locale which complies with ISO 3166. By default, the **us** locale is used and the call-progress tone, ring and cadence would be recognizable to US phone users.
4. At this point, FXS and FXO configuration differs:
5. *FXS:* configure ring frequency. In this context, we are not configuring how often a ring is given (which is configured in the **cptone** command) but the frequency in Hertz that is used to ring the telephone equipment. Use the **ring frequency** *frequency* command, where *frequency* can be either 25/50 Hz or 20/30 Hz depending on the equipment.
6. *FXO*: configure dial type with the option being either tone or pulse. The dial type is configured using the **dial-type** *pulse* | *tone* command.
7. Optionally, with FXS, you can change the ring cadence with the **cptone** command. Cadence can be altered individually or a new pattern can be created by using the **ring cadence** command.

E&M

1. As with FXO and FXS, enter voice-port configuration mode with **voice-port**.
2. Configure the access signaling type. On an E&M port, signaling types are wink-start, immediate-start or delay-start. Use the **signal** *wink-start* | *immediate-start* | *delay-start* command.
3. Configure call progress tones as in FXO/FXS, above, with **cptone** *locale*.
4. Configure the E&M port to use either 2 wires or 4 wires with **operation** *2-wire* | *4-wire*.
5. Finally, the type of E&M interface must be identified with **type** *1* | *2* | *3* | *4* | *5*.

Configuring Digital Voice Ports

Codec Complexity Configuration

Most Cisco equipment requires that the complexity of the codecs be configured before the rest of a port's configuration is completed. This configuration limits the type of codec that can be used on a specific voice-card. The voice-card uses this configuration to determine the total number of calls which can be active without oversubscribing the circuit being configured. There is some hardware available that allows what is called *flex* mode. In flex mode, it is possible to configure a number of channels which exceeds the capability of the hardware if all the channels being used require the higher complexity codec. This type of configuration does require oversubscription; if a number of calls come up and all require the higher complexity codec, the DSP will be unable to devote the resources to enable any more calls and actively drops new calls until the resources are freed.

Codec complexity can be configured with either DS0 or PRI groups. This configuration requires the voice-card configuration mode. While in the voice-card configuration mode use **codec complexity** *high* | *medium* | *flex* to set codec complexity.

Controller Clocking Configuration

One of the first things that must be understood about digital circuits is that timing is very important. As digital T1 and E1 channels work by interleaving channel data at specific intervals the source of timing on both the sending and receiving sides must be the same. If this timing is off the receiving end will interpret the data as coming from a different channel then the sender thus making the data unusable.

There are two main types of clock used on Cisco equipment, internal and line. Cisco equipment has an internal clock which can be used for network timing. While the clock is useful it is not overly accurate (from a timing perspective). For this purpose it is often best to use the clock from the line going to the telephone CO, their timing comes from a global timing source of extreme accuracy. Networking equipment can be configured to take timing from only one source at a time; if multiple line sources are available then these sources must be prioritized. To change the clocking type for a T1/E1, use the **clock source** command.

Controller Configuration

1. Card type (T1/E1) is configured with **card type** *t1* | *e1 slot*.
2. Specific controllers on the cards can now be configured individually.
3. Enter controller configuration mode with **controller** *t1* | *e1 slot/port*.
4. Configure framing type on the specific controller. For T1 circuits, the command used to specify framing is the **framing** *sf* | *esf* command. Where *sf* specifies Superframe and *esf* specifies Extended Superframe. For E1 circuits, the command used to specify framing is the **framing** *crc4* | *no-crc4* | *unframed*. Where *crc4*specifies the CRC4 mechanism in G.704 being used, *no-crc4* specifies the CRC4 mechanism in G.704 is not being used and *unframed* specifies no framing used.
5. Configured clock source with **clock source** *{**line** primary}* | *internal*. In order to specify the use of the internal clock the *internal* keyword is used. When the line is to be used for timing the **line** keyword is used. If more than one line clock is specified than the *primary* keyword should be added with the **line** keyword to specify the correct line as primary.
6. Configured the line code. For T1 circuits, the command **linecode** *ami* | *b8zs* is used. Where *ami* specifies Alternate Mark Inversion and *b8zs* specifies Mark Inversion using eight-zero substitution.
7. Finally, create either a DS0 or a PRI channel group. The channel group is used to specify a number of channels with the same configuration parameters. Enter controller configuration mode.

Create a DS0 channel group with:

```
ds0-group ds0-group-number timeslots timeslot-list type {e&m-delay-
dial | e&m-immediate-start | e&m-wink-start | fxo-ground-start | fxo-
loop-start | fxs-ground-start | fxs-loop-start}
```

This command not only specifies the type of each port in the channel group but also the type of access signaling type.

The PRI channel group creates a PRI ISDN group; this requires a little more configuration then the DS0 channel groups.

1. Configure the ISDN switch-type; there are a number of different switch types.
2. Create the PRI group with **pri-group timeslots** *timeslot-range*.
3. Configure the signaling PRI channel. With T1s, this channel is 24; E1s use 16. This is done through the **interface** *interface interface-number* command, where T1s channel 24 would be specified with :23 and E1s channel 16 would be specified as :15 (For Example, **interface serial 0/0:23**).
4. Finally, while in interface configuration mode, in order for the traffic to be routed to the DSP, enter **isdn incoming-voice voice**.

Channel Group Voice Configuration

In order to configure the specific voice port the same configuration can be used which is referenced in the analog port configuration section including the **type**, **cptone**, **ring frequency**, and **ring cadence** among other commands.

The Function and Operation of Call-Legs

A call-leg is defined by Cisco as a connection to or from a voice gateway from a POTS or VoIP source. This is illustrated below:

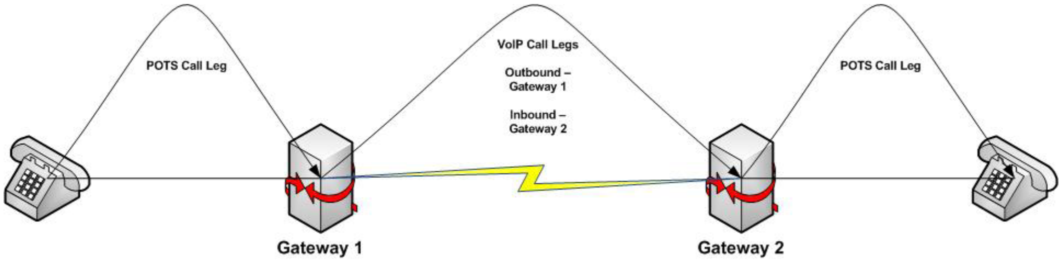


Figure 31: Call Legs

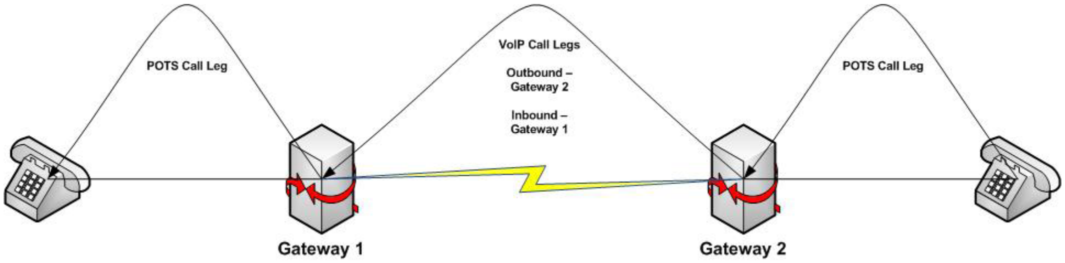


Figure 32: Call Legs - In Reverse Direction

This works by having an inbound and an outbound call leg central to each gateway. In a typical two-way connection there will be four call legs.

Configuring Dial Peers

Dial peers are the physical representation of the logical Call Legs. A Dial Peer is an addressable endpoint and is used to setup the parameters used to complete a call. These parameters can include calls based on called number, calling number, and entry port as well as a variety of different options which include the codec used and IP destination. There can be multiple dial peers which can be matched based on many of these parameters.

There are four main dial peer types including POTS, VoIP, VoFR and VoATM although focus is typically put on POTS and VoIP for the test. POTS dial peers are what connect to a traditional PSTN network through either analog or digital ports. The POTS peer is configured to provide an address (or addresses) to be used for the port and configures the physical port that is assigned these addresses.

The VoIP dial peer is used to connect to IP Networks through any IP enabled interface or port. The VoIP dial peer is responsible for providing a routing mechanism for specifically configured addresses (telephone numbers).

Basic Dial-Peer Configuration

All types of dial peers that can be configured on Cisco equipment is done through the same basic syntax. This includes the use of the **dial-peer voice** *number* **{pots | voip}** command which is issued in global configuration mode. The *number* in this case simply identifies the dial-peer on the equipment.

Assigning Voice Ports

When using POTS dial peers it is necessary to assign a specific voice port so that traffic that is matched to the POTS peer knows which port to use. This assignment is done with the **port** *port-id* command which is issued in dial-peer voice configuration mode. How the *port-id* is used greatly depends on the type of equipment being used and the type of port which is in use.

Specifying Session Targets

When using VoIP dial peers it is necessary to specify a session target which is simply the remote device which will be sent traffic should the dial-peer be matched. The command that is used to specify this session target is the **session-target ipv4:***ip-address* | *hostname* (when using VoIP) which is issued in dial-peer voice configuration mode. If the dial-peer is a VoIP peer then the target will be the IP address or hostname of the remote router; this IP address or hostname must be able to be reached through normal routing protocols for the VoIP dial peer to establish.

Destination Pattern Matching

In order to match a specific dial peer a destination pattern is used. When a POTS dial peer is used the destination pattern is used to match the traffic to a specific port, when using a VoIP dial peer the traffic is matched to a specific session target. The command that is used is **destination-pattern** {**+**} *string* {**T**}, which is used while in dial-peer voice configuration mode. The '+' which can be used within the **destination-pattern** is used when the pattern being matched is a standard E.164 address. The *string* parameter can be very complex but here are the most used options. The *string* itself is typically used as a match parameter against the called phone number and can be simply an exact matched phone number. However, what is typically done is a match is based on the preceding digits in a phone number. In order to match these digits a couple common matching parameters are used. The period (.) character is used to match any specific valid single character, brackets ([]) can be used to indicate a specific range and the **T** character can be used to indicate a variable length dial string which can end with any type of character. For example, if you are trying to route all traffic which is in the 212 area code and using the 555 prefix then you would match '212555T' or '212555….'.

As a side note it should be known that the use of the **T** character as a variable match causes a dial delay, when this is used there is a 10 second dialing delay while the equipment waits for additional digits.

Configuration Example

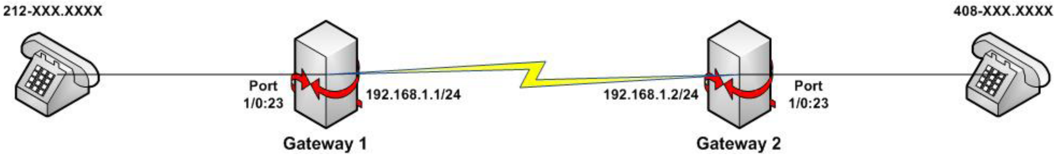
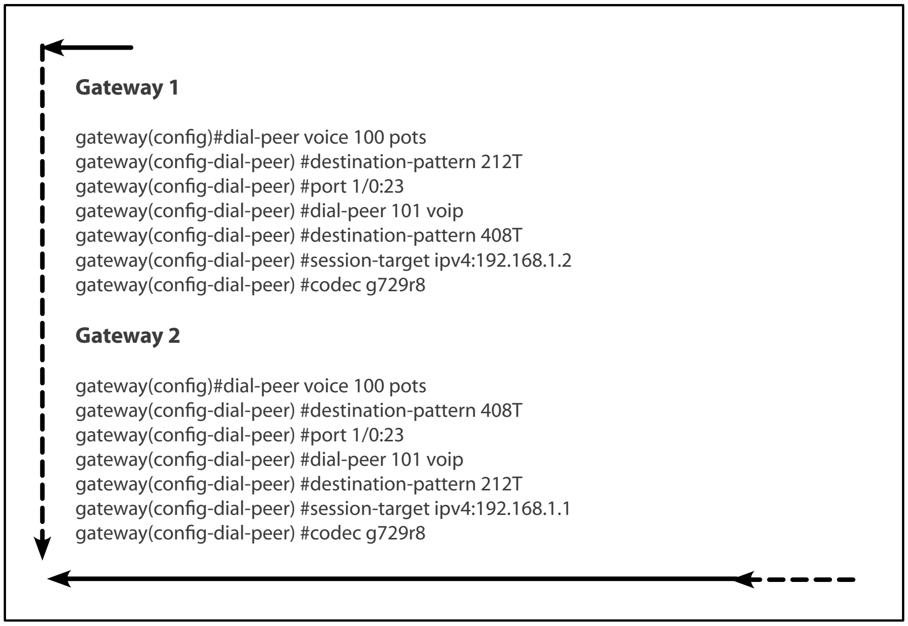


Figure 33: Dial-Peer Configuration Topology



Gateway 1

```
gateway(config)#dial-peer voice 100 pots
gateway(config-dial-peer) #destination-pattern 212T
gateway(config-dial-peer) #port 1/0:23
gateway(config-dial-peer) #dial-peer 101 voip
gateway(config-dial-peer) #destination-pattern 408T
gateway(config-dial-peer) #session-target ipv4:192.168.1.2
gateway(config-dial-peer) #codec g729r8
```

Gateway 2

```
gateway(config)#dial-peer voice 100 pots
gateway(config-dial-peer) #destination-pattern 408T
gateway(config-dial-peer) #port 1/0:23
gateway(config-dial-peer) #dial-peer 101 voip
gateway(config-dial-peer) #destination-pattern 212T
gateway(config-dial-peer) #session-target ipv4:192.168.1.1
gateway(config-dial-peer) #codec g729r8
```

Figure 34: Dial-Peer Configuration Example

The above illustrates a simple Dial-Peer example. In this example there are two different communities which are connected together through an IP network, one which services the 212 area code and the other which services the 408 area code. In the configuration for gateway 1 and 2 the port connecting to these communities is 1/0:23. Each of the connecting gateways has an interface connecting to each other which uses the 192.168.1.0/24 network. Each of the gateways is configured with a VoIP dial-peer configuration which provides the remote gateways IP address to send VoIP traffic to. The final part of the configuration is to specify the codec to be used over the VoIP link; in this case the codec selected was based on G.729.

Domain 5 – Configuring a Cisco Network to Support VoIP

The Purpose of VLANs in a VoIP Environment

VLAN Purpose

A Virtual LAN (VLAN) is a way to segment a physical network into many logical segments which are then able to use the same physical infrastructure but not have contact with one another. Each VLAN that is configured has its own broadcast domain and its own IP subnet. When used for a VoIP deployment typically the voice and data networks occupy different VLANs, this allows them to not only be separate from each other which provides security but also allows the network to easily prioritize the voice traffic over the data traffic.

VLAN Trunking Protocol (VTP)

One of the ways to ease the deployment of VLANs across a wide network infrastructure is using VTP which is a Cisco proprietary protocol. What VTP provides is a way to propagate VLAN information across a number of different switches across the network thus preventing the extra configuration that would be required on each individual switch to configure each VLAN without it. VTP works by defining roles to each of the switches in the network, these roles are:

- **VTP Server** –in server mode, any VLAN configuration done on this switch will propagate across to all of the other participating VTP switches.
- **VTP Client** – in client mode, all updates are relayed to the switch but the switch is unable to add, delete or modify VLANs
- **VTP Transparent** – in transparent mode, the switch does not participate in VTP and simply ignores the VTP traffic, it does however relay VTP information across to other switches.

VTP keeps its configuration maintained through the use of a Revision number system. When a change is initiated on the VTP network it is propagated, when each switch updates its configuration the revision number is incremented by 1. The VTP server advertising the highest revision number is always considered the most updated. The last sentence brings up a caveat to the VTP system. If a switch being used on another network is inserted into an existing VTP network with a higher revision number, its VLAN configuration will then replicate to all VTP switches; if this was not intended, the effect can quickly create a large problem. Make sure that all new switches which are inserted into an existing VTP network are cleared of their existing VLAN configuration and all VTP revision databases are cleared and deleted. There are also two different main versions of VTP which can be used, version 1 and version 2, the main difference being support for token ring networks. By default, Cisco switches are configured to run version 1.

In order for a switch to join the VTP network it must have a couple main pieces of information, these include:

- VTP Version
- VTP Domain Name
- VTP Password (If Configured)

If any of these parameters do not match, these switches will not be able to communicate with the other switches.

VLAN Trunking

On a normal access switchport it is only able to be configured with one data VLAN and one voice VLAN; this can be a large issue when there are multiple switches in a network. This is why trunking switchports exist. When a switchport is configured in trunking mode then it is able to carry all of the VLANs configured across to other switches.

There are two different types of trunking available: **Inter-Switch Link** (ISL) and **802.1Q.** ISL is a Cisco proprietary method and is typically not used that much anymore. 802.1Q is the standardized method which defines a trunking port. 802.1Q works by tagging VLAN traffic so that all of the switches involved are aware of the correct VLAN it is assigned to.

VLAN Routing

One thing that needs to be understood about VLANs is that they are truly separate and cannot relay traffic between each other without the use of a layer 3 device. In some cases this device is the switch itself. If the switch supports layer 3 routing and in other configurations a router is configured with a trunk port connected to the switch to route between VLANs, this configuration is also referred to as Router-On-A-Stick.

Configuring a Switched Infrastructure to Support Voice and Data VLANs

VLAN Configuration

The configuration of VLANs on a switch is rather easy and involves using VLAN configuration mode. In order to enter VLAN configuration mode you use the **vlan** *vlan-id* command to create or modify a VLAN.

Once in VLAN configuration mode, you can name the specific VLAN for easy identification with **name** *vlan-name*.

In order to delete a VLAN, use **no vlan** *vlan-id*.

VTP Configuration

As discussed in an earlier section, in order for VTP to work correctly between switches a switch must be configured with a VTP mode, VTP version, VTP domain and an optional VTP password.

1. As there are three different available VTP modes the following commands can be used to configure the appropriate mode: **vtp mode** *server | client | transparent*
2. Next, configure the VTP version; by default, the VTP version is set to 1. The following commands are used to change the VTP version: **vtp version** *1 | v2-mode*
3. Next, you'll need to configure the VTP domain; the domain can be from 1 to 32 characters and is case sensitive: **vtp domain** *domain*
4. Optionally, you can create a password. This password can be from 1 to 32 characters long and is case sensitive: **vtp password** *password*.

Switchport Configuration

Access Port

1. The configuration of an access port on a switch is each to configure, simply force the port into access mode with **switchport mode access.**
2. Once a port is entered into access mode, it can then be configured with a specific VLAN and voice VLAN with **switchport access vlan** *vlan-id* and **switchport voice vlan** *vlan-id*.

Trunking Port Encapsulation

Cisco switches support ISL and 802.1Q, as mentioned previously. Configure trunking port encapsulation with **switchport trunk encapsulation** *isl* | *dotq1*.

When a trunking port is configured to negotiate its encapsulation it will always prefer ISL.

Mode

There are two different ways which can be used to configure a trunking port:

- Statically configuring the port as a trunk
- Configuring it to use Dynamic Trunking Protocol (DTP)

In order to statically configure the port, enter **switchport mode trunk**.

When using DTP, the two connecting switches negotiate trunking and, if both are in appropriate modes for trunking, a trunk will establish. There are two different dynamic trunking modes: **auto** and **desirable**. When a switchport is configured in auto mode it is able to become a trunk but only if it is initiated by the remote site. When a switchport is configured in desirable mode it will actively try to bring the trunk up. The following table shows which local and remote switchport modes are required for a trunk to come up.

	switchport mode trunk	switchport mode auto	switchport mode desirable
switchport mode trunk	trunk	trunk	trunk
switchport mode auto	trunk	access	trunk
switchport mode desirable	trunk	trunk	trunk

Table 5: DTP Trunking Modes

Describing the Purpose and Operation of PoE

Power over Ethernet (PoE) was developed to provide a device powering ability in locations where physical power is either restricted or not available. Essentially, a device is plugged into the network and this network cable is then used for both network connectivity and for power to run the device. There are two different methods of providing power on Cisco devices, proprietary and standard (802.3af and 802.3at, respectively).

Cisco's proprietary PoE solution is called **Cisco Inline Power** (ILP) and has the ability to support up to 15.4 watts of power per port. Cisco inline power beings work when it detects a device being plugged into a port. Once this happens the switch will send a Fast Link Pulse (FLP) tone signal, if the device requires power it will loop this tone signal back to the switch. At this point the switch will provide the minimal amount of power over the port (6.3 watts). With this amount of power the device boots and then communicates its actual power requirements via Cisco Discovery Protocol (CDP). If CDP is disabled the switch will automatically provide the maximum of 15.4 watts to the port.

The standard way of providing power came after Cisco inline power and works a little differently. First thing to mention is that the older standard is 802.3af and also provides up to 15.4 watts of power, a new standard 802.3at (PoE Plus) has since been ratified and can provide up to 25 watts of power per the standard (Some manufactures are saying they will provide more (Up to 90 watts as of this writing) using this standard). Both of these standards have a similar detection mechanism. The switch will have a small constant current which is applied to each line; this current will not hurt equipment which does not support PoE. Once the switch detects a device a pulse is sent over the line to detect a specific amount of resistance on the line which is built into each device. A specific resistance specifies the class of device on the port and thus the amount of power to provide, these classes are detailed below. With the new 802.3at standard a second pulse is used to specify the device as a Class 4 device (802.3at).

Power Classes	Power Allocated (Used)
Class 0	15.4 W (0.44W to 12.95W)
Class 1	4.0 W (0.44W to 3.84W)
Class 2	7.0 W (3.84W to 6.49W)
Class 3	15.4W (6.49W to 12.95W)
Class 4	25.0 W (As of this writing, unknown)

Table 6: 802.3af and 802.3at Power Classes

Factors That Impact Voice Quality

Voice quality over IP networks is a moving target, as it depends on a number of different factors. It must be decided, based on the availability of these factors and the expected quality of calls, what the correct codec to use on a given network actually is. The main factors that need to be analyzed are bandwidth, delay, jitter and loss.

Bandwidth

Bandwidth is simply the amount of data that can be sent over a network at one time. Bandwidth is the easiest part of QoS to understand, to use more bandwidth then is available on the network will cause some or all of the traffic to be affected. When thinking of bandwidth in QoS terms it is typically the available bandwidth that needs to be concerned with. Available bandwidth is a measurement of the minimum bandwidth available on a path from point A to point B divided by the number of potential traffic flows. This is shown in the following figure:

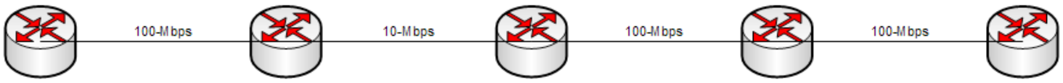


Figure 35: Bandwidth Example

Using this figure the amount of minimum bandwidth is 10-Mbps across the whole path, if ten flows are needed then the total available bandwidth per flow is 1-Mbps.

Delay

Delay is a crucial part of QoS management. The amount of overall delay from end-to-end is very important when dealing with voice and video over networks. Optimally, the delay for a VoIP network should be less than 150 ms. There are many different things that can affect the amount of delay that is introduced from one side of a path to the other. The four main delay factors are processing delay, queuing delay, serialization delay, and propagation delay.

- **Processing delay** – the amount of time that it takes the layer 3 devices (router or switch) to transfer a packet in one interface and out another. Many different things affect this including CPU speed, CPU utilization, total memory, available memory, and bus speed among others.
- **Queuing delay** – the amount of time that a packet spends in the queue of a layer 3 device. Queues are used in equipment to store data when the bandwidth is currently completely utilized; this information is stored for a short time in a queue until the bandwidth opens up. The amount of time that the packet spends in these queues is the queuing delay.
- **Serialization delay** – the amount of time that it takes for a packet to be broken down into layer 2 frames then into layer 1 electric or optical signals.
- **Propagation delay** – the amount of time it takes for a packet to cross the physical medium.

Jitter

Jitter or delay variation is when the amount of delay changes from packet to packet which causes packets to arrive at the destination out of order as determined by the Real-Time Protocol (RTP) time-stamping. Obviously, when dealing with a voice or video call the packets must be reassembled in the correct order or the voice or video would not make any sense. Some devices have what is called a jitter buffer which is used to mitigate small amounts of jitter by essentially creating a small queue of out of order packets and reorganizing them back into order. This can only be done correctly when the overall amount of jitter is minimal. This jitter buffer also adds additional end-to-end delay.

Loss

Loss is simple; it is the complete loss of a packet somewhere across the path from A to B. There are a number of different reasons for loss which include, output drop, input drop, overruns, ignored frames, and frame errors among others.

- **Output drop** (tail drop) – when a router is trying to transfer a packet from an input queue to an output queue after routing and finding the output queue to be completely full. If this happens, the packet is dropped.
- **Input drop** – when a router tried to receive a packet but its input queue is completely full.
- **Overruns** – when a router is trying to receive a packet but the router is so busy that it is unable to allocate buffer space for the packet. This does not mean that the buffer is full, simply that the CPU did not have the time to create it.
- **Ignored frames** – frames which are dropped because there was no level 2 buffer space available to put them.
- **Frame errors** – when a frame is received but the CRC or checksum do not match which shows that the frame was corrupted in some way along the link.

How QoS Addresses Voice Quality Issues

The **Quality of Service** (QoS) mechanism allows devices that transfer VoIP traffic to prioritize that traffic over any other traffic on the network. When everything works as it is supposed to, voice traffic is allowed a path across the network. This is accomplished in one of two ways: **integrated services** and **differentiated services**.

When using the integrated services model, all network elements must be aware of the QoS mechanism and be able to track their resources. When an endpoint attempts to make a call it requests a specific traffic profile which it needs to successfully complete a quality call. The network will then check to see if every device across the path is able to provide the profile elements required, if so the call is began and the resources are allocated. The problem with this type of model is that all network elements must be aware of the QoS requirements and must be able to communicate this for every call which can be a complex task.

When using differentiated services, traffic is classified into a specific priority and is marked with this information. Once the traffic is initially marked each device across the network gives appropriate priority to the traffic. When using this model trust boundaries must be setup so that traffic is correctly classified and marked. If data is classified then it may not receive the required priority to keep a quality call across the network.

AutoQoS

Cisco has also provided a method for implementing QoS without requiring a large amount of QoS knowledge through the use of AutoQoS. AutoQoS is a newer feature of Cisco IOS. It enables the router to monitor the traffic being processed across the router's interfaces and automatically setup traffic classes, policies and automatically enables them per interface. AutoQoS does this by monitoring the traffic on the router and watching for specific behavior, once it has enough information it will automatically create the IOS configuration that suits the need of the traffic. AutoQoS is designed to setup QoS specifically for voice traffic.

Domain 6 – Implementing UC500 Using Cisco Configuration Assistant

Cisco Configuration Assistant (CCA) Requirements

In order to run CCA on a computer there are a couple of minimal requirements which must be met, these include:

- Processor : 1Ghz
- DRAM : 512 MB minimum, 1024 MB recommended
- Hard-Disk Space : 150 MB Minimum, 300 MB Recommended
- Number of Colors : 65536
- Resolution : 1024 x 768

Anyone with a Cisco CCO account can download the CCA software which is available at http://www.cisco.com/go/configassist.

CCA Interface

There are a number of different main interfaces which are used when configuring a device with CCA. The following shows the main attributes of the CCA GUI interface:

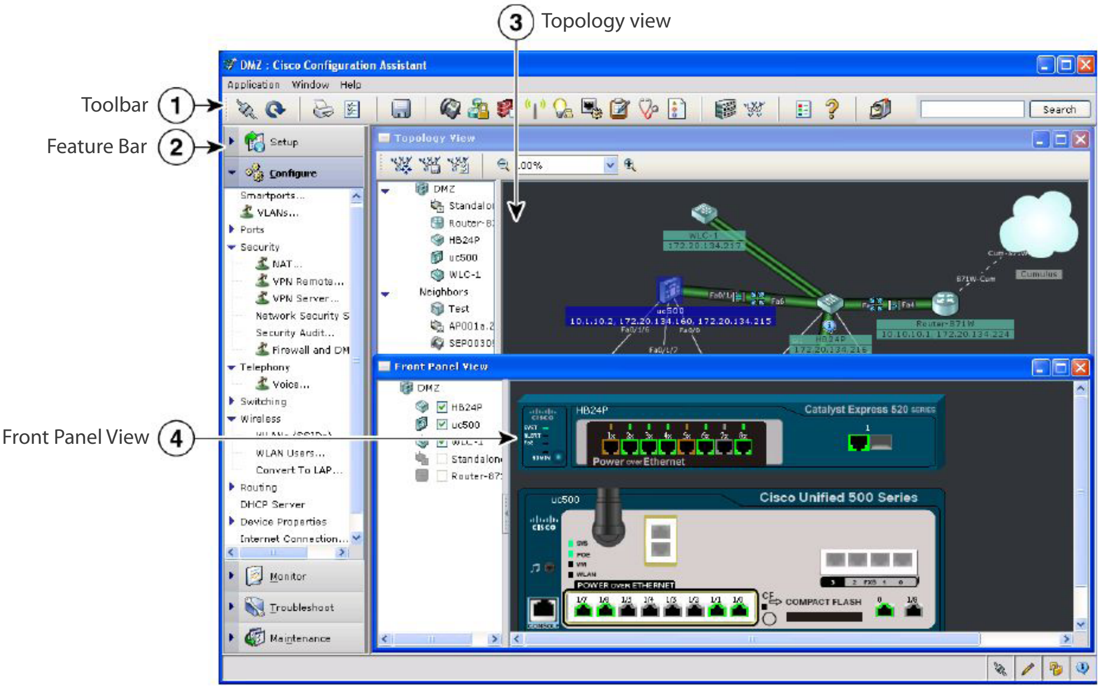


Figure 36: Main CCA GUI Interface

The following shows the front panel view which is available to show logical representation of the physical device:

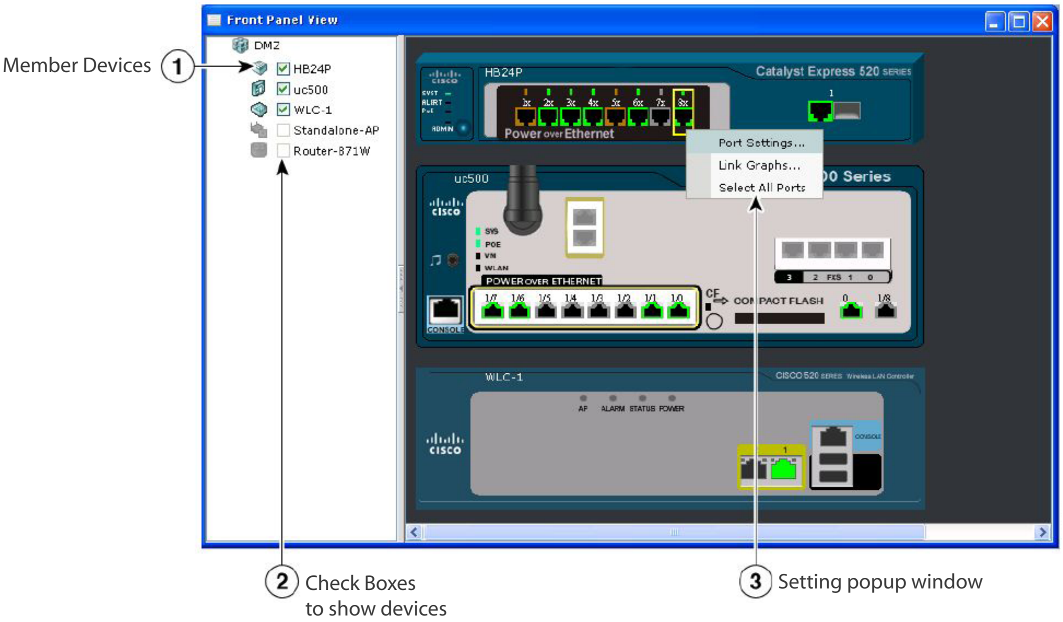
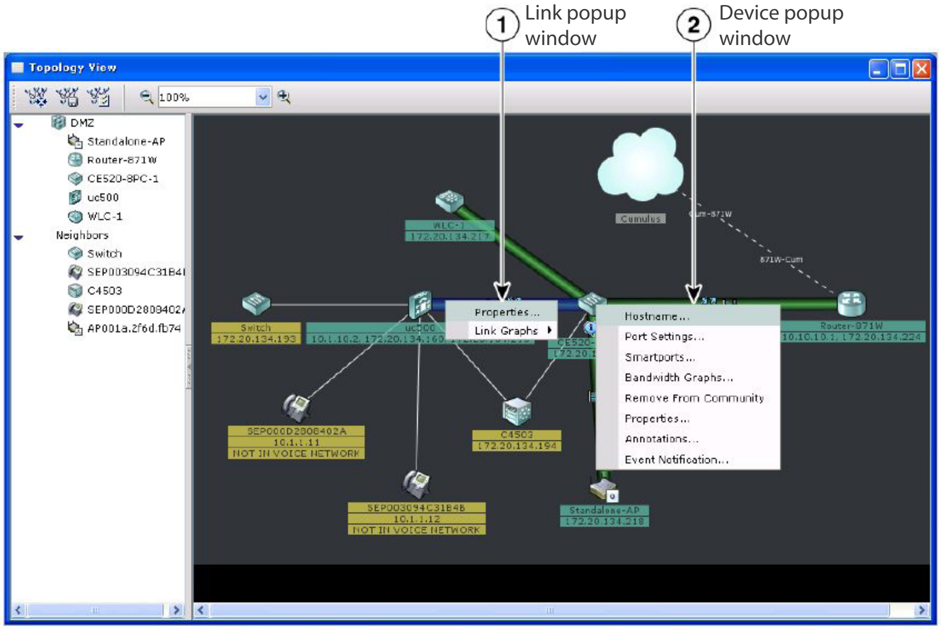


Figure 37: CCA Front GUI View

There is also an available topology view which is created as devices are added or discovered:



1 Link popup window

2 Device popup window

Figure 38: CCA Topology GUI View

In order to configure and view the various settings which are available to the user both the tool bar and feature bar are used. The following shows a picture of the feature bar which is available to the user:

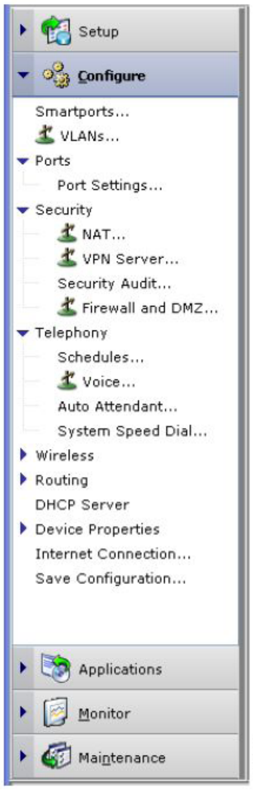


Figure 39: CCA Feature GUI Bar

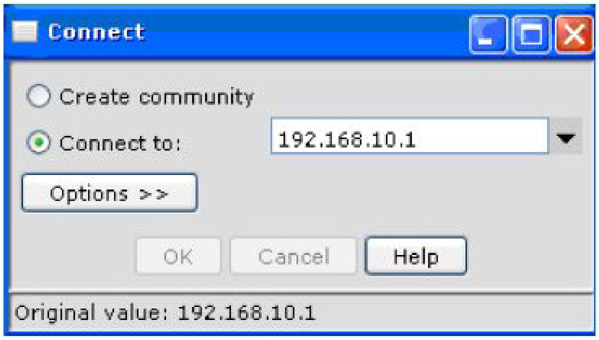
There is also a tool bar which is used to reach the various screens which can be used to configure the devices:

Connect	🔌
Refresh	⟳
Print	🖨
Preferences	☑
Save Configuration	💾
Voice	☎
VPN Server	🔒
Firewall/DMZ	🧱
Wireless Networks	📶
Smartports	💡
Port Settings	⚙
Inventory	📋
Health	🩺
Event Notification	⚠
Front Panel	▦
Topology	⋈
Legend	☰
Help	?
Feedback	📬

Figure 40: CCA Menu Bar Buttons

CCA Communities/Customer Sites

With CCAv1, there is a group of devices referred to as a "community" and can be used to easily group together devices which when combined provide the UC solution for a specific location. CCAv2 and use this concept, but instead of being called a community it is now referred to as a "customer site". The first step, which is accomplished when using CCA, is to establish a connection with a device. This can be done in a standalone manner or by creating a new community/customer site or opening an existing community/customer site. The following shows the connect dialog which is used when trying to connect to a device:



○ Create community

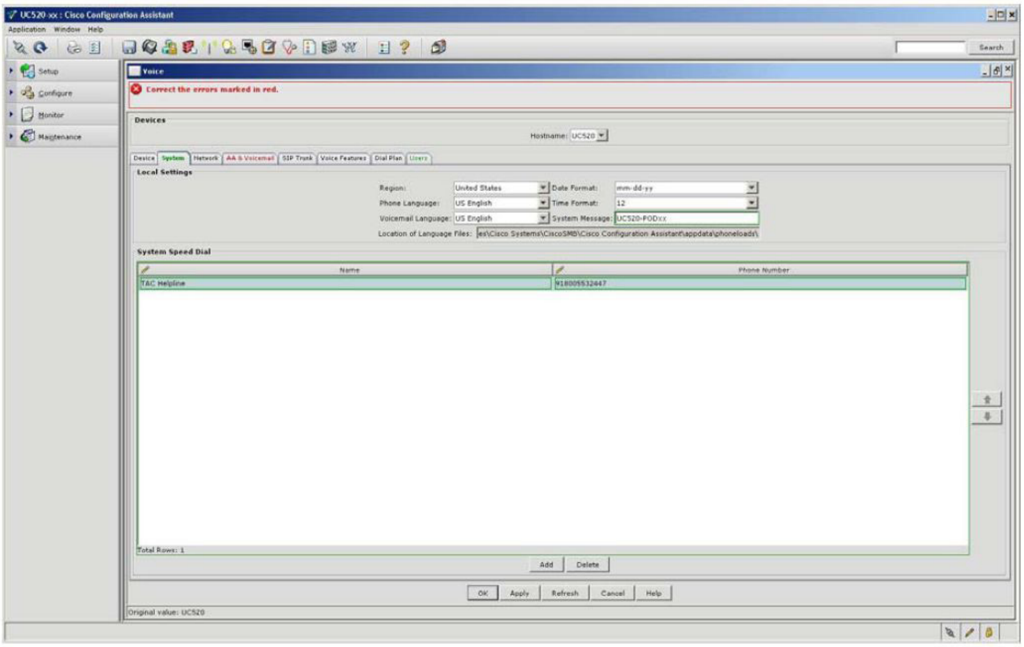
● Connect to: 192.168.10.1

Original value: 192.168.10.1

Figure 41: CCA Connect Dialog

CCA Voice Configuration Screens

There are a number of different voice configuration screens which are used to configure the various features which are available from each specific device. In order to get to each of these screens the feature bar or the menu bar as shown above is used. The following figures show a number of the main screens which are used to configure the main features:



Correct the errors marked in red.

Hostname: UC520

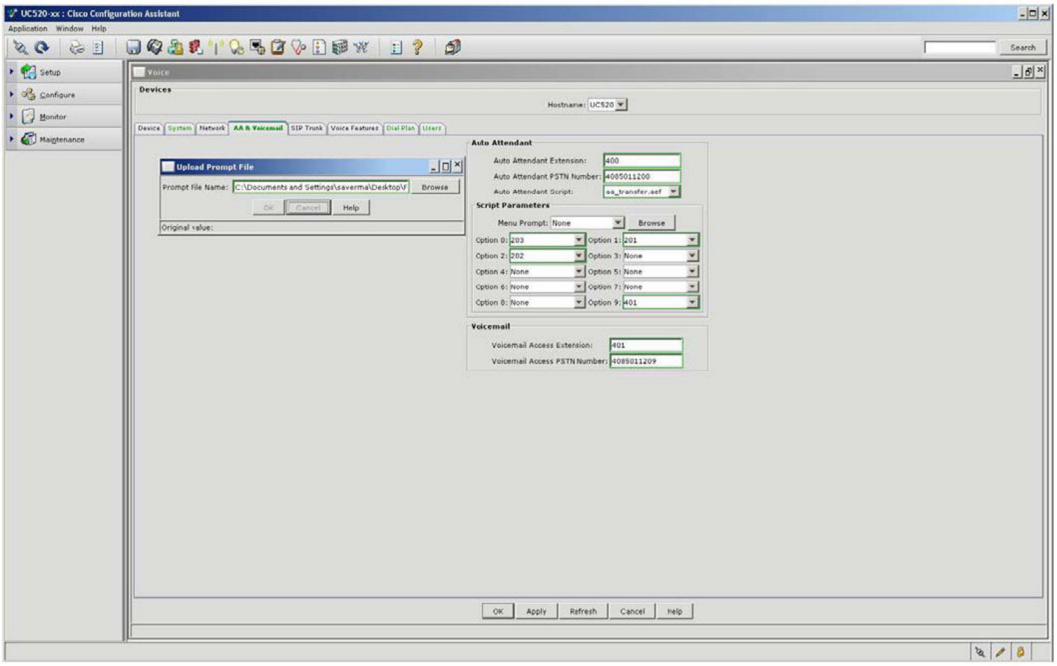
Region: United States
Date Format: mm-dd-yy
Phone Language: US English
Time Format: 12
Voicemail Language: US English
System Message: UC520-PODxx
Location of Language Files: es\Cisco Systems\CiscoSMB\Cisco Configuration Assistant\appdata\phoneloads\

Name	Phone Number
TAC Helpline	918005532447

Total Rows: 1

Original value: UC520

Figure 42: CCA Voice - System Tab



Hostname: UC520

Upload Prompt File

Prompt File Name: C:\Documents and Settings\saverma\Desktop\F

Original value:

Auto Attendant

Auto Attendant Extension: 400

Auto Attendant PSTN Number: 4085011200

Auto Attendant Script: aa_transfer.aef

Script Parameters

Menu Prompt: None

Option 0: 203 Option 1: 201

Option 2: 202 Option 3: None

Option 4: None Option 5: None

Option 6: None Option 7: None

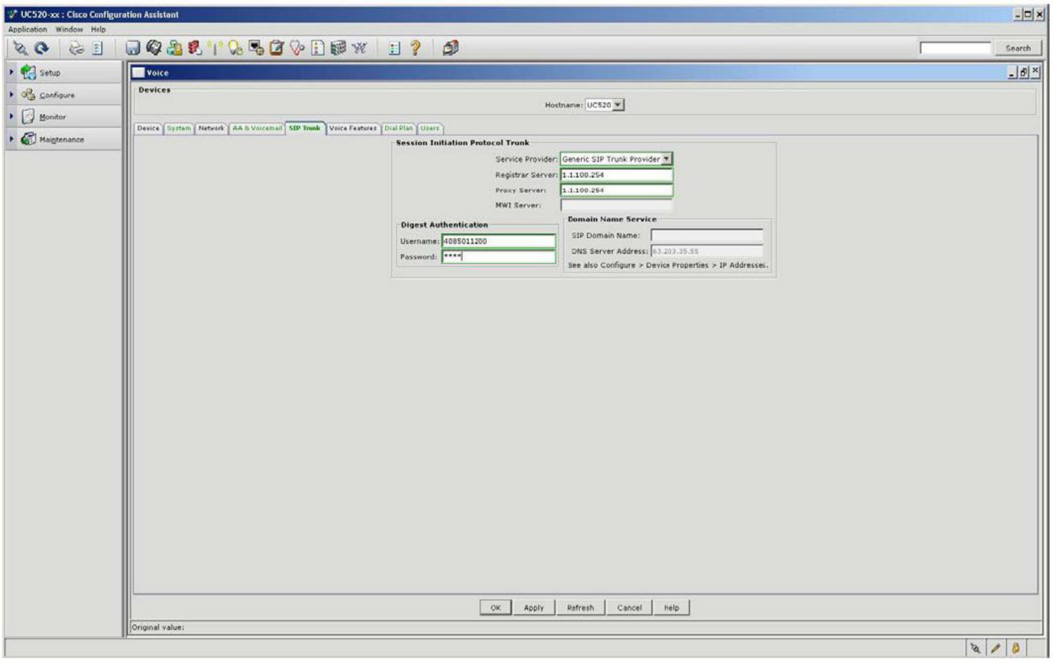
Option 8: None Option 9: 401

Voicemail

Voicemail Access Extension: 401

Voicemail Access PSTN Number: 4085011209

Figure 43: CCA Voice - AA (Auto Attendant) and Voicemail Tab



Hostname: UC520

Session Initiation Protocol Trunk

Service Provider: Generic SIP Trunk Provider

Registrar Server: 1.1.100.254

Proxy Server: 1.1.100.254

MWI Server:

Digest Authentication

Username: 4085011200

Password: ****

Domain Name Service

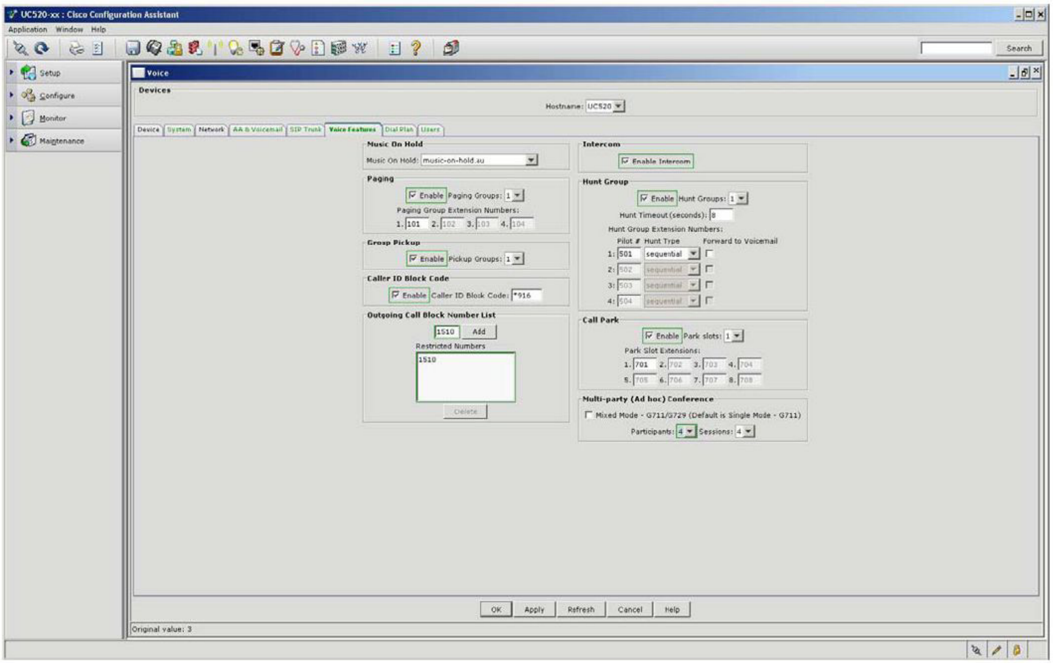
SIP Domain Name:

DNS Server Address: 63.203.35.55

See also Configure > Device Properties > IP Addresses.

Original value:

Figure 44: CCA Voice - SIP Trunk Tab



Hostname: UC520

Music On Hold

Music On Hold: music-on-hold.au

Paging

☑ Enable Paging Groups: 1

Paging Group Extension Numbers: 1. 101 2. 102 3. 103 4. 104

Group Pickup

☑ Enable Pickup Groups: 1

Caller ID Block Code

☑ Enable Caller ID Block Code: *916

Outgoing Call Block Number List

1510

Restricted Numbers

1510

Intercom

☑ Enable Intercom

Hunt Group

☑ Enable Hunt Groups: 1

Hunt Timeout (seconds): 8

Hunt Group Extension Numbers:

	Pilot #	Hunt Type	Forward to Voicemail
1:	501	sequential	□
2:	502	sequential	□
3:	503	sequential	□
4:	504	sequential	□

Call Park

☑ Enable Park slots: 1

Park Slot Extensions: 1. 701 2. 702 3. 703 4. 704 5. 705 6. 706 7. 707 8. 708

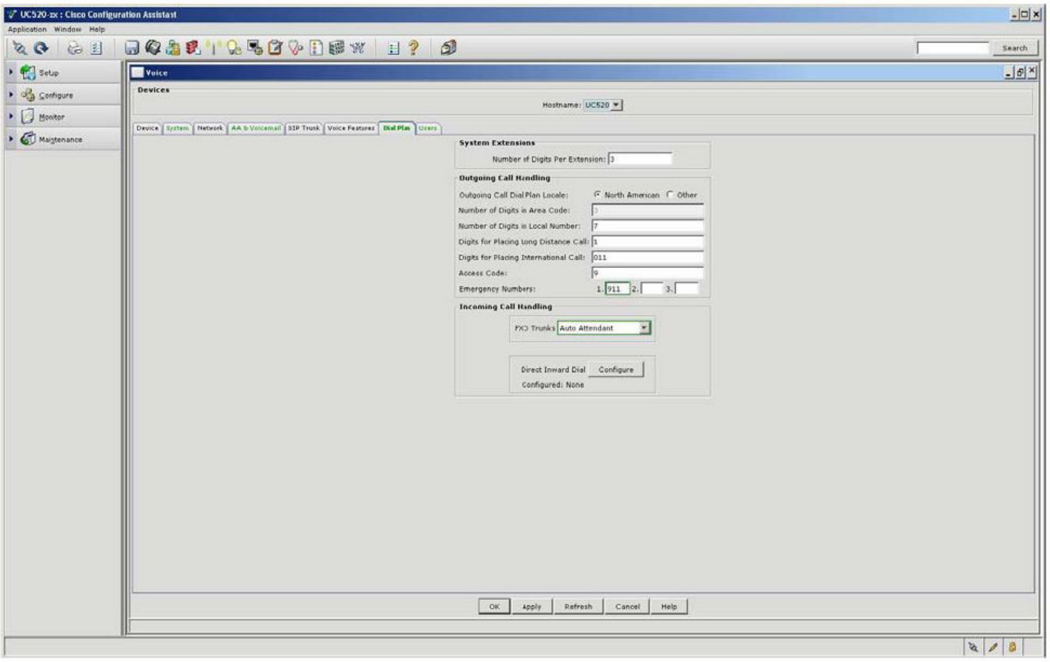
Multi-party (Ad hoc) Conference

□ Mixed Mode - G711/G729 (Default is Single Mode - G711)

Participants: 4 Sessions: 4

Original value: 3

Figure 45: CCA Voice - Voice Features Tab



Hostname: UC520

System Extensions

Number of Digits Per Extension: 3

Outgoing Call Handling

Outgoing Call Dial Plan Locale: ● North American ○ Other

Number of Digits in Area Code: 3

Number of Digits in Local Number: 7

Digits for Placing Long Distance Call: 1

Digits for Placing International Call: 011

Access Code: 9

Emergency Numbers: 1. 911 2. 3.

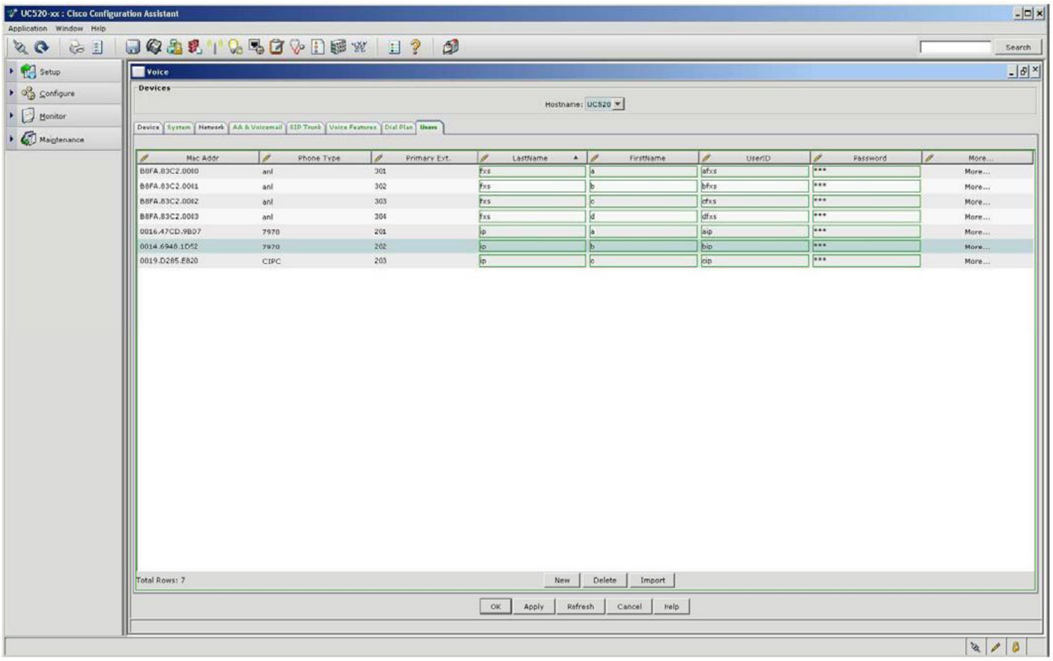
Incoming Call Handling

FXO Trunks Auto Attendant

Direct Inward Dial

Configured: None

Figure 46: CCA Voice - Dial Plan Tab



Mac Addr	Phone Type	Primary Ext.	LastName	FirstName	UserID	Password	More...
B8FA.83C2.0080	anl	301	fxs	a	afxs	***	More...
B8FA.83C2.0081	anl	302	fxs	b	bfxs	***	More...
B8FA.83C2.0082	anl	303	fxs	c	cfxs	***	More...
B8FA.83C2.0083	anl	304	fxs	d	dfxs	***	More...
0016.47CD.9BD7	7970	201	ip	a	aip	***	More...
0014.6948.1D52	7970	202	ip	b	bip	***	More...
0019.D285.E820	CIPC	203	ip	c	cip	***	More...

Figure 47: CCA Voice - Users Tab

Domain 7 – Implementing Cisco Unified Communications Manager Express (CME)

Describe the appropriate software components needed to support endpoints

Licensing

The first thing that must be understood is the licensing requirements for CME. There are three different types of license:

- **IOS License** – The IOS must be able to support CME features
- **Feature License** – A feature license (seat license) grants the router a specific number of IP phones
- **Phone User License** – Each phone must also have a license attached to each device, this is typically sold with every new phone.

IOS

The first step of implementing CME is the installation of a CME supporting IOS version to the specific device. This is done in the same way that all IOSs are installed on Cisco devices: through the use of TFTP to transfer the image to the device. Depending on the device, it may support multiple images or just one at a time. Read over the specific device documentation to find the specifics if each CME supporting device.

CME Files

All of the CME files are also transferred onto the supporting device. There are a number of different files which must be transferred. These files are separated into a number of categories and the files which are required for each specific implementation can be transferred without having to transfer the files which will not be used. These categories include:

- **Basic files** – these are the core CME files, these include a set of phone firmware files.
- **GUI files** – these are the files which are required to run the web-based GUI.
- **XML template file** – this file is used to dictate the structure of the web-based management utility.
- **MOH files** – these are the audio files which are used for Music on Hold (MOH)
- **Script files** – various Tool Command Language (Tcl) scripts used to supply additional functionality.
- **Miscellaneous files** – additional files which can be used to provide additional functionality like custom ringtones and different backgrounds for IP phones.

Once these files are transferred to the CME device the device must then be configured to operate as a TFTP server so that the files specific to each connecting IP phone can be transferred on phone boot up.

Requirements and Settings for DHCP, NTP and TFTP

DHCP

Whenever configuring a DHCP server for use with CME endpoints, there is a specific option which is required by these endpoints to be correctly configured. This option is 150 and is used to specify the TFTP server to be used by the CME endpoints. TFTP is used to transfer configuration files to Cisco IP phones. The other DHCP parameters which are configured are more typical ones, including a default gateway and DNS server(s).

NTP

The Network Time Protocol (NTP) is vital in order to maintain clock synchronization between the various devices in your UC network. These include the clocks as shown on the IP phones, voice-mail tags, Call Detail Records (CDR), and device logging timestamps.

Cisco uses a hierarchy for clock sources: this starts with a stratum 1 source, which is considered the most accurate. Any source that gets its clock information from a stratum 1 source is then referred to as a stratum 2 source; sources that get their information from a stratum 2 source are then a stratum 3 source. There are a number of different publically available sources which can be used to source your NTP network. Public sources are typically stratum 2 or 3 sources and are still quite accurate. The other option is to buy equipment to directly clock your network from a master source like GPS. This equipment will then output a stratum 1 equivalent source.

TFTP

The general setup for a TFTP server is rather straightforward; however, the acting TFTP server in a CME network is usually the router itself. Because of this, the device must be configured to serve the appropriate phone files.

Configuring DHCP, NTP and TFTP

DHCP

In order to configure DHCP a couple pieces of information must be known first, these include:

- IP Addresses to be issued
- Default Gateway
- DNS Server(s)
- Excluded IP Addresses from Range

1. The first step is to configure any excluded IP addresses. This is done first so that addresses from the range are not given out before the included IP ranges are configured. The command to configure the excluded IP address is:

   ```
   ip dhcp excluded-address low-address [high-address]
   ```

2. When using this command, either enter a specific IP address or specify a range. When only a specific IP address is desired, omit the *high-address* parameter.

3. The second step is to create a DHCP pool. Once in DHCP pool configuration mode, various options can be configured to be used with the pool. The following command is used to create the DHCP pool:

   ```
   ip dhcp pool pool-name
   ```

4. The third step is to specify the specific addresses range given out to the endpoints; the command to configure this is as follows:

   ```
   network network-subnet network-subnet-mask
   ```

5. The fourth step involves configuring the various options which are given out with the IP address to the endpoint. Remember the one option which is unique to this DHCP server setup is the use of the option 150 to specify the TFTP server. The following are the commands which are used to configure these options:

   ```
   default-router ip-address
   dns-server ip-address
   option 150 ip ip-address
   ```

NTP

The first thing that must be completed when configuring NTP is to enter a command which points to the NTP source. The command to do this is as follows:

```
ntp server ip-address | hostname
```

Since publically available clocks are set to the Universal Time Coordinated (UTC) time zone, it is necessary to set the time zone of the device. The command which is needed to set the time zone is:

```
clock timezone zone hours-offset minutes-offset
```

The *zone* parameter is used for display purposes and can be up to 7 characters. The *hours-outset* and *minutes-offset* parameter is used to set the number of hours to offset the displayed clock, the device itself keeps the clock in UTC format and uses these parameters to display the time in your region.

Another issue when configuring NTP is the use of daylight saving time (DST). In order to accurately display the time on these devices during this time, use the following command:

```
clock summer-time zone recurring [week day month hh:mm week day month
hh:mm [offset]]
```

The *zone* parameter in this command is the same as with the above command and is used for display purposes. The *week, day, month and hh:mm* parameters are configured depending on your specific DST settings. The *offset* parameter is optional and defaults to 60 minutes. For example, in the United States the clocks go ahead by 1 hour (60 minutes) on the second Sunday in March and go back an hour on the first Sunday in November. The correct command to set for the east coast in the US would be:

```
clock summer-time EDT recurring 2 Sunday March 2:00 first Sunday
November 2:00
```

TFTP

TFTP server configuration on a Cisco device is rather simple; the following command is used for each file:

```
tftp-server flash [partition-number:]filename1 [alias filename2]
```

The specific *partition-number* and directory structure used in the *filename1* parameter will depend on your specific installation. The use of the **alias** parameter is optional but is typically used to make the request of specific files easier as the request only requires a filename and not the directory structure. The following example shows how to configure to serve a file which is located under the phone/7900 directory called firmware.bin:

```
tftp-server flash:/phone/7900/firmware.bin alias firmware.bin
```

Differences between Key Systems and PBX Mode

There is a basic difference between how a key system is designed and how a PBX system is designed. A key system is designed like older phone systems, where each line that comes into the office is ported to a specific line on each phone in the office. In this configuration, all of the lines coming into an office go to all of the phones in the office.

When designing a system like a PBX, each phone is given an extension which must first dial an access code to use an outside line (typically an 8 or 9). In this configuration inbound calls are routed through an auto attendant or physical receptionist who routes the call to the correct extension.

The Different Types of ePhones and ePhone-DNs

ephone

An **ePhone** (more commonly written in all lower case letters, ephone) represents a physical IP phone or softphone used to receive and dial calls. Each of these phones is configured on the router and identifies using the MAC address of the phone being configured.

ephone-dn

An **ePhone-DN** (more commonly written in all lower case letters, ephone-dn) is used to represent a single or dual line directory number, each of these numbers can be associates so that it is used as one of the buttons the ephone being configured. During the configuration of the ephone-dn is when an extension or direct full phone number is assigned. There are two different ways to configure an ephone-dn, single-line or dual-line. This distinction is simple if you are familiar with modern normal phone lines as a single-line is a line which is unable to deal with more than one call at a time. A dual-line is able to deal with two simultaneous calls at the same time when using features like call-waiting or conferencing.

Configuring Cisco Unified Communications Manager Express Endpoints

Basic CME Configuration

The first thing that must be configured on a CME router is the number of ephone and ephone-dns which will be supported. Bypassing this step is not possible as, by default, each of these is set to zero and thus not configured to support any ephone or ephone-dns. There are two commands used to set the number of ephone and ephone-dns and both are entered while in telephony service configuration mode.

```
telephony-service
max-ephones max-phones
```

Next, the association of each model of phone, with its respective firmware file (transferred and set up per the TFTP server configuration) must be configured. This is done with the following command:

```
load phone-type firmware-file
```

The *phone-type* in this case being the specific phone which will be used with CME and the *firmware-file* is the name of the filename of the firmware itself without the .bin extension.

After associations are configured, the IP address which will be used to source traffic to and from the IP phones must be set up. Typically, this is set up to be either the gateway IP address if the router is the gateway to all of the phones; or, it is set to a loopback IP address on the router when the router is used by multiple subnets. The command to set this source IP address to be used is as follows:

```
ip source-address ip-address
```

CME Endpoint Configuration

This next section reviews the basic commands which are used to setup a simple CME endpoint, a more detailed review is out of the scope of this guide.

ephone-dn

There are two basic commands which need to be understood for a basic CME configuration. The first command is used to create an ephone-dn and the second is used to configure a specific number which is associated with the created ephone-dn. The commands to accomplish these are as follows:

```
ephone-dn dn-tag [dual-line]
number number [secondary number]
```

ephone

For an ephone there are three main commands which must be configured. The first command is used to create the ephone, the second is used to associate a specific phones MAC address to the ephone and the third is used to setup the buttons on the ephone. The commands to accomplish these are as follows:

```
ephone phone-tag
mac-address mac-address
```

While the **ephone** and **mac-address** commands are straight forward, the **button** command is not. The *physical-button-number* is straightforward and relates the physical button on the ephone referenced. The *separator* parameter is used to specify how the button behaves. The basic values of the *separator* parameter are ':', 'c', and 'o'. The ':' represents a normal ringing phone, the 'c' represents a line which is configured for call waiting and allows a second overlaid ephone-dn and an 'o' represents an overlay line which is allowed to be overlaid with up to 25 ephone-dns.

Configuring Call-Transfer per Design Specifications

There are two different methods of call transfer, Consult and Blind. When using the Consult method: you press the 'Trnsfer' key, dial the number, speak with the party and hit the key again to connect the two calls and drop off the line. When using the Blind method: you press 'Trnsfer' key and dial the number, the call will automatically be connecting and you are dropped off the line. The Consult method requires a second line or a dual-line ephone-en to work.

The method to be used is configured system-wide; the command to change this is as follows:

```
transfer-system {full-blind | full-consult}
```

Configuring Voice Productivity Features

Hunt Groups

Hunt groups are simply configured by assigning the same extension to a number of ephone-dns. In order to control specific hunt behavior, the **huntstop** command is used. This command is detailed as follows:

```
huntstop [channel]
```

The **huntstop** command by itself tells the router to stop looking for other destination matches (If you have a dual line ephone-dn it will give the called party a call waiting beep). The **huntstop channel** command changes this by stopping the hunt if a single channel is currently busy (if you are on the phone on a dual line phone the caller would get a busy signal). Another option is to enable the **huntstop channel** command and the **no huntstop** command (In that order) which will tell the system to hunt to other ephone-dns for matches should the called party already be on a call.

Call Park

In order for call park to work, there must either be spare ephone-dns configured which are not assigned to a specific ephone or there must be ephone-dns setup specifically for call parking.

In order to setup an ephone-dn to be used for call park you use the **park-slot** command.

Call Pickup

The call pickup feature allows a group of phones to pick up another ringing IP phones call when the 'PickUp' key is pressed. This is a common feature in an office where outside parties have the direct extensions of inside phones. If a phone is ringing in a specific group and another member of the group wants to pickup that call without going to that person's desk this is what the call pickup feature does. In order to configure this, the following command is used on each ephone-dn in a group:

```
pickup-group group-number
```

Paging/Intercom

Paging

When paging is used, a number can be dialed to broadcast to configured phones. This is configured by creating an ephone-dn which is dedicated for paging. Once this is complete each phone is configured to be used with that paging ephone-dn. The commands to accomplish this are **paging** for an ephone-dn and **paging-dn** *dn-tag* for a regular ephone.

Intercom

An intercom is a simple connection which is typically configured between two phones. In order to configure this to work two new ephone-dns must be configured for each side of the connection. It is recommended that the number which is configured on the ephone-dn be something that can't be dialed into from an IP phone console, as this limits the ability to call into an intercom which is not typically wanted; the use of a letter in the **number** command is allowed to provide this. The second part of the configuration involves a command to automatically call the other side of the intercom, by default when configured as an intercom the remote IP phone will auto-answer the phone and mute it allowing the person on the line to hear you but you not to hear them. The commands which are used to provide this functionality are as follows:

```
intercom dn-tag [barge-in [no-mute] | no-auto-answer | no-mute]
[label label]
```

This command is entered on both sides in the ephone-dns configuration. In order to change the default intercom behavior of auto-answering with mute enabled, the **barge-in**, **no-auto-answer**, or **no-mute** options can be used. The **barge-in** option will automatically place any existing call on the called side on hold before causing the intercom to answer. The **no-auto-answer** option causes the intercom button to ring the remote side instead of auto-answering. The **no-mute** option will auto-answer the remote side without mute enabled.

Configuring Music on Hold (MoH)

There are three different ways to configure MoH: external jack, multiple unicast streams or a single multicast stream. When using the US500 series an external jack can be used as a MoH source. When not using the UC500 series external jack, the command used to enable MoH and assign a specific music file is **moh** *filename*.

The file which is used must be transferred to the flash of the router and must be in .au or .wav format and have 8-bit 8-kHz data in A-law or mu-law data.

In order to configure the use of a single multicast stream, the following command is used:

```
multicast moh ip-address port port-number
```

The ip-address can be any multicast address which is not in the 224.x.x.x range. For the port-number is recommended that 2000 be used as it is the common RTP port number, however any number from 2000 to 65535 can be used.

Domain 8 – Implementing Voicemail Features Using Cisco Unity Express

Available Features in Cisco Unity Express

VoiceMail

The following features are provided by Cisco Unity Express for voicemail:

- **Users and Groups** – used to define the users on the system and to group them according their function in the company. Groups are either a collection of users or other groups.
- **Support for both Subscriber and General Delivery mailboxes** – both individual (subscriber) mailboxes and group (general delivery) mailboxes are supported.
- **Additional Mailbox subscriber features** – there are a number of subscriber features provided including greetings, message management, message waiting indicator, message notifications and distribution lists to name a couple.
- **Additional Mailbox caller features** – there are a number of caller features provided including various record message options, operator assistance and mailbox login.
- **VoiceView Express** – feature which allows an IP phone to provide a "visual" voicemail ability through the phone screen.
- **Integrated Messaging** – provides the ability to retrieve messages through a phone system, VoiceView Express or through email.
- **Voice Profile for Internet Mail (VPIM)** – provides the ability to transfer voicemail message between different systems through an email type of facility.

AutoAttendant

The following features are provided by Cisco Unity express for AutoAttendant:

- **Cisco Unity Express Automated Attendant** – provides the mail functionality of the AutoAttendant allowing the direction of calls through an automated system
- **Cisco Unity Express Custom Scripting** – provides the ability to customize all parts of the AutoAttendant experience, through the programming of various software steps.

Configuring Cisco Unified Communications Manager Express to Support Cisco Unity Express

There are a number of steps which must be completed in order to have Cisco Unity Express work with Cisco Unified Communications Manager Express. These steps are detailed as follows:

1. Configure Service Engine
2. Download and Install Software
3. Addition of licensing files
4. Configuring HTTP and Authentication
5. Configuring Dial-Peer
6. Configuring Telephony Service

Configuring the Service Engine

When the Unity Network Module (NM) or Advanced Integration Module (AIM) are inserted into a router a Service Engine interface will show up as configurable in the configuration. This Service Engine must be configured in order for Unity Express to work correctly. The first thing that must be done is the configuration of an IP address; this is done through the normal **ip address** command. Typically, the Service Engine is given an unnumbered IP address which it shares with another interface in the router; this is usually a loopback interface. Use **ip unnumbered** *interface* to configure this.

The *interface* parameter is the interface which is sharing its IP address. The second thing that needs to be configured is the service module IP address. Now this sounds confusing as there are two different IP addresses being used, think of the Service Engine IP address as the external interface to the service modules internal IP address. Along with assigning an IP address to the service module it must also be configured with a default gateway. The commands to perform this are as follows:

```
service-module ip address ip-address subnet-mask
service-module ip default-gateway ip-address
```

The IP address that should be used is in the same subnet as the Service Engine and the gateway configured should be configured to the IP address of the Service Engine. The final thing that needs to be configured for the IP routing to work correctly is the creation of a static route which points all traffic to the service modules IP address to the Service Engine interface. The commands to perform this are as follows:

```
ip route service-module-ip-address 255.255.255.255 service-engine-
interface
```

Download and Install Software

There are two main commands which are used to download and install the Unity Express software, these commands are as follows:

software download {clean | upgrade} **url** *url*

software install {clean | upgrade} **{pkg** *package-name* | **url** *url*}

The FTP protocol is used to transfer the files from a server to the Unity Express hardware, the *url* parameter which is used in both of these commands is used to specify the location of the files to be downloaded. When using the **software download** command the files are transferred for installation at another time. When this is done the **pkg** *package-name* parameter of the **software install** command is used to install. If you want to install the package directly from the server the **software download** command is not needed as the **software install** command will download and install the file.

Adding Licensing Files

In order for Unity Express to operate it must be properly licensed, this is done through the transfer of a license file using the previous sections commands.

Configuring HTTP and Authentication

The main way to configure Unity Express is through a web interface, in order to make sure that CME and Unity Express work together some configuration is required to make sure this interface is working correctly. The following commands are used to enable this functionality:

```
ip http server
ip http path file-path
ip http authentication authentication-method
```

The *file-path* parameter is used to specify the location of the proper files; this is typically sent to **flash**. The *authentication-method* is typically set to **local** or **aaa** depending on whether you are using the locally configured user authentication database of an Authentication, Authorization and Accounting (AAA) server.

Configuring Dial-Peers

The dial-peer configuration is used to allow CME to correctly access Unity Express when the functionality is required. There are three dial-peers which are required: one for VoiceMail, Auto Attendant and Administration via Telephone (AvT). The commands required for this are detailed below; the entire dial-peer configuration is the same between the three except for the destination-pattern match:

```
router(config)#dial-peer voice extension voip
router(config-dial-peer)#destination-pattern pattern
router(config-dial-peer)#session protocol sipv2
router(config-dial-peer)#session target ipv4:service-module-ip-address
router(config-dial-peer)#dtmp-relay sip-notify
router(config-dial-peer)#codec c711ulaw
router(config-dial-peer)#no vad
```

Which pattern you use for each service is determined by the **ccn trigger** commands entered for Unity Express. This amount of detail is out of the scope of this document.

Configuring Telephony Service to Activate Unity Express Voicemail

The final thing that must be configured to have CME utilize Unity Express is the configuration of the

Telephony service. The commands used are as follows:

```
router(config-telephony)#voicemail voicemail-number
router(config-telephony)#web admin system name username secret password
router(config-telephony)#dn-webedit
router(config-telephony)#time-webedit
```

The *voicemail-number* is the number which is dialed when the voicemail button is pressed on the IP phones. The **web admin system** command is optional and is used to allow a single portal for both Unity Express and CME; the credentials used here are for access to the CME GUI. The **dn-webedit** command is optional and allows the Unity Express GUI to edit the CME directory numbers. The **time-webedit** command is optional and is used to allow the Unity Express GUI to manually change system time.

Practice Questions

Chapter 1

1. What types of communication devices can the Cisco Unified Communications Express handle? Choose three:

   ❍ A. Software phones

   ❍ B. Video devices

   ❍ C. Instant Messaging

   ❍ D. Hardware Phones

   ❍ E. Cellular Phones

2. What type of QOS is not supported on the Cisco Unified IPT network solution? Select the best answer.

   ❍ A. Traffic shaping

   ❍ B. Compressed Real-Time Transport Protocol (cRTP)

   ❍ C. Low-latency queuing

   ❍ D. Beaconing

3. What are the two main functions of the Cisco Unity Express module?Choose two:

   ❍ A. Voice mail

   ❍ B. Auto Attendant

   ❍ C. Call Processing

   ❍ D. Web services

4. What is not a benefit of using the distributed call processing design model? Select the best answer.

   ❍ A. PSTN call savings when using the IP WAN for calls between sites

   ❍ B. Scalability

   ❍ C. Increased utilization of WAN bandwidth

   ❍ D. Increased number of PSTN lines at each site

Chapter 2

1. What type of multiplexing uses arbitrary number of variable bit-rate digital channels that is often used in packet-oriented communication? Select the best answer.

○ A. Time division multiplexing

○ B. Statistical multiplexing

○ C. Frequency division multiplexing

○ D. PRI

2. On traditional POTS network, what information does the telephone network use to route calls to a specific destination?Select the best answer.

○ A. MAC address

○ B. Destination IP Address

○ C. Telephone numbering plan

○ D. FECN

3. Choose the components that make up the North American Numbering Plan local number. Choose three:

○ A. Country code

○ B. PBX extension

○ C. Line number

○ D. Central office code

○ E. Area Code

Chapter 3

1. What are the voice payload sizes for the G.711 and G.729 codecs? Select the best answer.

○ A. G.711 = 80 bytes
G.729 = 10 bytes

○ B. G.711 = 160 bytes
G.729 = 20 bytes

○ C. G.711 = 4 bytes
G.729 = 4 bytes

○ D. G.711 = 2 bytes
G.729 = 2 bytes

2. Using the given analog sound wave diagram, which part of the sound wave depicts the amplitude? Select the best answer.

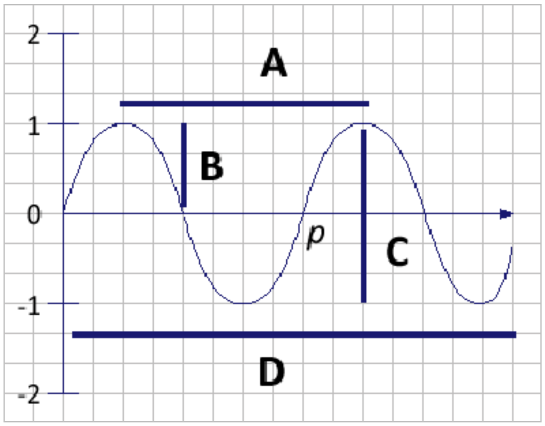
❍ A. Letter A

❍ B. Letter B

❍ C. Letter C

❍ D. Letter D

Exhibit(s):



3. What protocol does a Cisco switch utilize to tell the IP phone how it should send voice traffic to the switch? Select the best answer:

❍ A. An IP Broadcast

❍ B. Cisco Discovery Protocol (CDP)

❍ C. An IP Multicast

❍ D. OSPF protocol

Chapter 4

1. Which dial string answer fits the destination string given below? Select the best answer.

55[4-6,9]25.6

❍ A. 5532516

❍ B. 554256

❍ C. 5572516

❍ D. 5592586

2. Which dial peer configuration will work to allow an access code of 9 and allows the user to be able to dial all local, long distance and international calls? Select the best answer.

❍ A. dial-peer voice 1 pots

destination-pattern 9.
port 1/0:1

❍ B. dial-peer voice 1 pots

destination-pattern 9#
port 1/0:1

❍ C. dial-peer voice 1 pots

destination-pattern 9$
port 1/0:1

❍ D. dial-peer voice 1 pots

destination-pattern 9T
port 1/0:1

❍ E. dial-peer voice 1 pots

destination-pattern 9%
port 1/0:1

3. What is a voice gateway responsible for doing? Choose two:

❍ A. Translates voice communication between dissimilar networks

❍ B. Functions exclusively within the Unified CallManager Express solution

❍ C. Translates analog-to-digital and digital-to-analog communication

❍ D. Maintains the phone directory database

4. Given the following dial string, what command needs to be added to forward all digits within the string to the PSTN? dial-peer voice 1 potsdestination-pattern 555...port 1/0:1
Select the best answer.

❍ A. no digit-strip

❍ B. No command is needed. The gateway will send all 7 digits to the

❍ PSTN.

❍ C. prefix 7

❍ D. forward-digits 3

Chapter 5

1. A customer is interested in deploying a new Cisco Unified Communications system on their current network. They already have a network that is using public address space. Unfortunately, there are not enough public IP addresses to support both the voice and data network. What benefits would be achieved for deploying a separate voice VLAN on the network? Choose two:

○ A. With a separate voice VLAN, you could deploy private (RFC 1918) address space on the phones to free up scarce public IP addresses

○ B. Adding a voice VLAN makes QOS easier to configure.

○ C. Each IP phone and PC will need a separate Ethernet connection.

○ D. Having a separate voice VLAN reduced Spanning-tree overhead

2. Looking at the show mls qos command for port fa0/1, what can you determine about how the trust state is configured on this switchport? Select the best answer.

○ A. Port fa0/1 will trust the DSCP priority sent from an IP phone.

○ B. Port fa0/1 will trust the CoS priority sent from an IP phone.

○ C. CoS override is enabled and will set all traffic to a CoS of 5

○ D. The trust boundary is pushed to the switchport level. The phone's CoS is not trusted.

Exhibit(s):

```
Switch#show mls qos interface fastEthernet 0/1

FastEthernet0/1
 trust state: trust cos
 trust mode: trust cos
 COS override: dis
 default COS: 0
 DSCP Mutation Map: Default Mutation Map
 trust device: none
```

Chapter 6

1. The Cisco Configuration Assistant provides the following functionality except. Select the best answer:

○ A. Simplified network reporting

○ B. Drag and drop software updates

○ C. Multiple network views

○ D. Load balancing

○ E. Troubleshooting

○ F. Simplified configuration for voice, data, security and wireless networks.

2. Which tab of the Cisco Configuration Assistant would you go to if you want to configure voice features such as: MOH, paging, hunt groups can call park? Choose the best answer:

○ A.The AA and Voicemail tab

○ B.The Voice Features Tab

○ C.The SIP Trunk tab

○ D.The System tab

Chapter 7

1. Given the ephone and ephone-dn partial configuration given, if three calls are placed to extension 5001 simultaneously, what happens to the third call? Select the best answer:

○ A.The call will ring on the second line of ephone 1.

○ B.The call will ring on the second line of ephone 2.

○ C.The call will ring on the second line of ephone 1 and 2.

○ D.The call will receive a busy tone

Exhibit(s):

```
ephone 1 dual- line
 button 1: 1
 mac-address 0030.12c3.8434

ephone-dn 1
 number 5001
 preference 0
 huntstop channel

ephone 2 dual- line
 button 1: 2
 mac-address 0030.24a2.325

ephone-dn 2
 number 5001
 preference 1
 huntstop channel
```

2. You are adding a new Cisco 7961 phone to your CME environment. You have the partial configuration in the router. What command is needed to associate the new phone to the ephone 1 configuration if autoregistration is disabled? Select the best answer:

○ A. Router(config)# ephone-dn1 dual-line

○ B. Router(config)# ephone 1
Router(config-ephone)# mac-address xxxx.xxxx.xxxx.xxxx

○ C. Router(config)# ephone 1
Router(config-ephone)# max-ephones 1

○ D. Router(config)# ephone-dn 1
Router(config-ephone-dn)# ephone-dn-template 1

Exhibit(s):

```
ephone-dn 1
 number 233

ephone-dn 4
 number 234

ephone-dn 16
 number 235

ephone-dn 19
 number 236

ephone 1
 button 1:192:43:16 4s1
```

3. What is the default SCCP protocol/port?Choose the best answer:

○ A. UDP 2000

○ B. Option 150

○ C. TCP 2000

○ D. Random TCP port over 1024

4. Which Unity Express capabilities are available with the telephone user interface (TUI)? Choose three:

○ A. Recording personal greetings

○ B. Modification of extension numbers.

○ C. Vacation or emergency notifications

○ D. Digit manipulation

○ E. Remote directory lookup

Chapter 8

1. What are the minimum router configuration steps needed to get Cisco Unity Express up and running? Choose three:

❍ A. Configure a static route pointing to Unity

❍ B. Assign an IP address to Unity

❍ C. Configure DHCP

❍ D. Assign an IP address on the router and configure routing.

❍ E. Configure EIGRP on Unity

2. Looking t the show voicemail command given, what does the "Zero Out Number" setting do? Select the best answer.

❍ A. When a caller is directed to a PrepLogic's Voicemail box, they can verbally say the number "0" to be redirected to extension 1234

❍ B. When a caller is directed to a PrepLogic's Voicemail box, they can press the 0 digit on their phone to end the call.

❍ C. When a caller is directed to a PrepLogic's Voicemail box, they can press the 0 digit on their phone to access the voicemail greeting.

❍ D. When a caller is directed to a PrepLogic's Voicemail box, they can press the 0 digit on their phone to be redirected to extension 1234

Exhibit(s):

```
se-10-0-0-0# show voicemail detial mailbox preplogic
Owner:                                 /sw/local/users/user3
Type:                                  Personal
Description:                           PrepLogic mailbox
Busy state:                            idle
Enabled:                               true
Mailbox Size (seconds):                480
Message Size (seconds):                180
Play Tutorial:                         true
Space Used (seconds):                  0
Total Message Count:                   0
New Message Count:                     0
Saved Message Count:                   0
Future Message Count:                  0
Deleted Message Count:                 0
Expiration (days):                     10
Greeting:                              alternate
Zero Out Number:                       1234
Created/Last Accessed:                 Aug 15 2008 18:31:15 PST
```

3. Looking at the show voicemail command given, what does the "Play Tutorial" setting do? Select the best answer.

○ A. The voicemail tutorial will start up for mailbox owners logging in to their mailbox for the first time. Once the user has gone through the tutorial, it will not play again. This command is enabled by default.

○ B. The voicemail tutorial will start up for mailbox owners logging in to their mailbox for the first time. Once the user has gone through the tutorial, it will not play again. This command is diabled by default.

○ C. The voicemail tutorial will start up for mailbox owners logging in to their mailbox for the first time. The tutorial will continue to play until it is disabled on the CallManager This command is diabled by default.

○ D. The voicemail tutorial is for system administrators only. A password must be entered to disable the tutorial on mailboxes.

Exhibit(s):

```
se-10-0-0-0# show voicemail detial mailbox preplogic
Owner:                                 /sw/local/users/user3
Type:                                  Personal
Description:                           PrepLogic mailbox
Busy state:                            idle
Enabled:                               true
Mailbox Size (seconds):                480
Message Size (seconds):                180
Play Tutorial:                         true
Space Used (seconds):                  0
Total Message Count:                   0
New Message Count:                     0
Saved Message Count:                   0
Future Message Count:                  0
Deleted Message Count:                 0
Expiration (days):                     10
Greeting:                              alternate
Zero Out Number:                       1234
Created/Last Accessed:                 Aug 15 2008 18:31:15 PST
```

Answers & Explanations

Chapter 1

1. Answers: A, B, D

Explanation A. Correct - Soft Phones are fully supported

Explanation B. Correct - Video Conferencing is supported

Explanation C. Incorrect - IM is not supported on the Unified Communications Express platform

Explanation D. Correct - Hard phones are fully supported.

Explanation E. Incorrect - Cell phones are not supported by the Cisco Unified Communications Express platform

2. Answer: D

Explanation A. Incorrect - Traffic shaping is a supported QOS mechanism.

Explanation B. Incorrect - cRTP is supported and works very well over low-bandwidth links.

Explanation C. Incorrect - LLQ is a popular method of prioritizing voice traffic.

Explanation D. Correct - Beaconing refers to token-ring networks and has nothing to do with QoS.

3. Answers: A, B

Explanation A. Correct - Cisco Unity Express is a distributed voice mail application.

Explanation B. Correct - The auto attendant provides businesses with way to transfer calls to various extensions without human interaction.

Explanation C. Incorrect - The CallManager Express handles call processing

Explanation D. Incorrect - the CME can handle simple web services.

4. Answer: D

Explanation A. Incorrect - This is one of the main benefits of a distributed model. Being able to utilize the IP WAN can dramatically cut down on PSTN costs.

Explanation B. Incorrect - The distributed model is far more scalable than the single-site model.

Explanation C. Incorrect - The WAN bandwidth a site has may be underutilized, adding voice traffic can take advantage of the wasted bandwidth without additional costs.

Explanation D. Correct - Increasing the number of PSTN lines raises the monthly costs to each site. The goal is to reduce the amount of calls placed on the PSTN and to utilize the IP WAN links instead.

Chapter 2

1. Answer: B

Explanation A. Incorrect - TDM allocates the same timeslot to every channel which can waste bandwidth if the channel is not being used. TDM is often used in PSTN communication such as standard T1 PRI voice circuits.

Explanation B. Correct - Statistical muxing can provide for more efficient use of a circuit when sending packet based data such as TCP or UDP communication.

Explanation C. Incorrect - This type of muxing is to divide up the sound spectrum among various channels. It is most often used in radio communication.

Explanation D. Incorrect - A Primary Rate Interface (PRI) is a physical medium with which to transport 24 POTS circuits from one point to another.

2. Answer: C

Explanation A. Incorrect - The MAC address is used on Ethernet, TokenRing, ATM and other more advanced networks.

Explanation B. Incorrect - Traditional telephony networks do not use IP.

Explanation C. Correct - a unique telephone number is attached at the CO switch level that uniquely identifies each subscriber line. This number is used to efficiently route the call to a destination subscriber line.

Explanation D. Incorrect - FECN deals with Frame Relay congestion avoidance and has nothing to do with standard PSTN networks.

3. Answers: C, D, E

Explanation A. Incorrect - The country code is not required when dialing a NANP local number

Explanation B. Incorrect - A PBX extension is not part of the NANP

Explanation C. Correct - the line number is the 4 digit number that is specific to the specific PSTN line.

Explanation D. Correct - This 3 digit number is unique for each CO

Explanation E. Correct - This 3 digit code is unique for a specific geographical region.

Chapter 3

1. Answer: B

Explanation A. Incorrect - 80 bytes for the G.711 and 10 bytes for the G.729 codecs are the sample sizes and not payload size

Explanation B. Correct - Address signaling is what the phone system uses to connect calls.

Explanation C. Incorrect - 4 bytes is the size of the payload with cRTP header compression and checksums

Explanation D. Incorrect - 2 bytes is the size of the payload with cRTP header compression

2. Answer: B

Explanation A. Incorrect - Letter A shows the wavelength

Explanation B. Correct - The amplitude is the height of the wave from point 0.

Explanation C. Incorrect - The amplitude is a measurement of a sound wave measured from the mean position to an extreme.

Explanation D. Incorrect - The amplitude is a measurement of a sound wave measured from the mean position to an extreme.

3. Answer: B

Explanation A. Incorrect - CDP is used to inform the IP phone what method it should send the voice traffic.

Explanation B. Correct - CDP packets are sent out the switchport to the phone to inform the switch on what method the switch expects voice traffic to be sent.
The choices are:

Voice VLAN tagged with a Layer 2 CoS priority value

Access VLAN tagged with a Layer 2 CoS priority value

Access VLAN, untagged

Explanation C. Incorrect - CDP is used to inform the IP phone what method it should send the voice traffic.

Explanation D. Incorrect - CDP is used to inform the IP phone what method it should send the voice traffic.

Chapter 4

1. Answer: D

Explanation A. Incorrect - The third digit must be either 4,5,6 or 9

Explanation B. Incorrect - This number is only 6 digits in length

Explanation C. Incorrect - The third digit must be either 4,5,6 or 9

Explanation D. Correct - The third digit is a 4,5,6 or 9 and the 6th digit is a wildcard 0-9 number

2. Answer: D

Explanation A. Incorrect - The string 9. Specifies that the dial peer supports only a 2 digit string.
The "." Is any number 0-9

Explanation B. Incorrect - The string 9# is not valid as the "#" wildcard is only for DTMF tones.

Explanation C. Incorrect - The string 9$ is not valid as the "$" wildcard is used in translation rules and not dial peers

Explanation D. Correct - The 9T string means that it accepts 9 as the first digit. The "T" wildcard matches any number of successive digits. This would allow a user to dial local, long distance and international numbers with a single dial-string.

Explanation E. Incorrect - The string 9% specifies that the dial peer supports the 9 digit first.
The "%" wildcard means that it accepts the preceding digit any number of times. Because the only digit preceding the "%" wildcard is 9, then this string would not work.

3. Answers: A, C

Explanation A. Correct - The gateways convert communication from one type to another.

Explanation B. Incorrect - Voice gateways are needed within every voice solution.

Explanation C. Correct - The gateways can terminate POTs lines and converts the signals from digital systems to analog lines and visa versa.

Explanation D. Incorrect - The phone directory is stored within the CallManager system

4. Answer: A

Explanation A. Correct - This command after a dial string forces the gateway to send the static digits "555" to the PSTN instead of just the wildcard numbers.

Explanation B. Incorrect - By default, only the wildcard digits will be forwarded to the PSTN

Explanation C. Incorrect - The prefix command would be used to add specific digits to the front of the dialed string before it is forwarded to the telephony interface. In this case, the number 7.

Explanation D. Incorrect - This command tells you how many digits to forward to the PSTN. In this example, the last 3 digits of the entire string would be forwarded.

Chapter 5

1. Answers: A, B

Explanation A. Correct - This is a great way to get around the limited public IP addresses as the IP phones likely do not need a public IP address.

Explanation B. Correct - by separating the voice traffic from the data, it allows for easier QOS configuration and implementation.

Explanation C. Incorrect - Cisco IP phones allow both the voice and data VLANs to be trunked. A single Ethernet connection is needed from the switch. The PC can then plug into the IP phone.

Explanation D. Incorrect - Adding a second VLAN for voice does not impact STP.

2. Answer: B

Explanation A. Incorrect - The port is a layer 2 connection and will understand and trust CoS values.

Explanation B. Correct - the command "mls qos trust cos" was configured on the interface.

Explanation C. Incorrect - COS override is disabled on the interface.

Explanation D. Incorrect - The trust state for the switchport is set to trust CoS coming from an IP phone.

Chapter 6

1. Answer: D

Explanation A. Incorrect - The configuration assistant provides GUI base network reporting tools

Explanation B. Incorrect - Drag and drop software updates simplify updates

Explanation C. Incorrect - The configuration assistant supports multiple views.

Explanation D. Correct - The Cisco Configuration assistant does not provide load balancing.

Explanation E. Incorrect - The configuration assistant has several tools to assist in troubleshooting.

Explanation F. Incorrect - This powerful GUI configuration tool assists in configuring all the mentioned network functions.

2. Answer: B

Explanation A. Incorrect - The Voice Features tab configures various voice features such as MOH, paging, hunt groups and others.

Explanation B. Correct - This screen is where you can configure various CME features.

Explanation C. Incorrect - The Voice Features tab configures various voice features such as MOH, paging, hunt groups and others.

Explanation D. Incorrect - The Voice Features tab configures various voice features such as MOH, paging, hunt groups and others.

Chapter 7

1. Answer: D

Explanation A. Incorrect - The "huntstop channel" command allows only 1 call to go tob the ephone-dn. The second channel on each phone is used for placing calls on hold or for outbound calls.

Explanation B. Incorrect - The "huntstop channel" command allows only 1 call to go to the ephone-dn. The second channel on each phone is used for placing calls on hold or for outbound calls.

Explanation C. Incorrect - The "huntstop channel" command allows only 1 call to go to the ephone-dn. The second channel on each phone is used for placing calls on hold or for outbound calls.

Explanation D. Correct - The "huntstop channel" command will only allow a single call. The first call will be sent to ephone 1 because of the lower preference. The second call will be sent to ephone 2. The third call will receive a busy signal.

2. Answer: B

Explanation A. Incorrect - The "dual-line" command allows for transfer of calls on the line. This will not help associate the ephone 1 configuration to the new 7961 phone

Explanation B. Correct - The MAC address is needed in the ephone 1 configuration to associate the 7961 phone to the config.

Explanation C. Incorrect - The "max-ehpones" configures the maximum number of Cisco IP phones that can be supported by a router.

Explanation D. Incorrect - The "ephone-dn-template" will import the template dn configuration of template 1. This will not help associate the ephone 1 configuration to the new 7961 phone.

3. Answer: C

Explanation A. Incorrect - SCCP communicates between the CallManager and the IP phones for call setup and teardown. It uses TCP 2000 by default.

Explanation B. Incorrect - Option 150 is a DHCP option to allow the IP phones to receive the IP address of the CallManager so they can download the configuration files via TFTP. It is not a port/protocol for SCCP.

Explanation C. Correct - SCCP runs along TCP 2000

Explanation D. Incorrect - SCCP communicates between the CallManager and the IP phones for call setup and teardown. It uses TCP 2000 by default.

4. Answers: A, C, E

Explanation A. Correct - Users can use their handsets to record personal greetings using TUI.

Explanation B. Incorrect - TUI does not have the ability for users to modify extension numbers.

Explanation C. Correct - Special vacation and/or emergency voice notifications can be made with TUI.

Explanation D. Incorrect - Digit manipulation is not possible with TUI.

Explanation E. Correct - Remote directory lookup can be used with TUI although it is disabled by default.

Chapter 8

1. Answers: A, B, D

Explanation A. Correct - A static route is necessary to get packets routed to Unity properly.

Explanation B. Correct - An IP address must be assigned to Unity so the router can send packets correctly to Unity.

Explanation C. Incorrect - While DHCP is often used, it is not one of the minimum router configuration requirements.

Explanation D. Correct - This is necessary to be able to communicate with Unity and other IP devices on the network.

Explanation E. Incorrect - Unity does not support EIGRP.

2. Answer: D

Explanation A. Incorrect - The user must press the number 0 on their telephone keypad.

Explanation B. Incorrect - The zeronumberout command redirects users to extension 1234 when the "0" key is pressed on the telephone keypad.

Explanation C. Incorrect - The zeronumber out command is used when a caller does not want to leave a voicemail and instead would like to talk to an operator at extension 1234.

Explanation D. Correct - The zeronumberout command specifies the extension where a caller is routed when the caller presses "0" to reach an operator after being transferred to a subscriber's mailbox.

3. Answer: A

Explanation A. Correct - The tutorial command enables the mailbox tutorial program when the telephone subscriber logs in to the voice-mail system for the first time. To disable this option, use the "no tutorial" command.

Explanation B. Incorrect - The tutorial is enabled on all mailboxes by default. To disable this option, use the "no tutorial" command.

Explanation C. Incorect - Once the mailbox owner goes through the tutorial for the first time, it will not play again. The tutorial is enabled on all mailboxes by default. To disable this option, use the "no tutorial" command.

Explanation D. Incorrect - The Voicemail tutorial is for general users that have a mailbox. The tutorial assists the user to setup various functions of their specific mailbox.