

CCIE Voice Written Exam Study Guide

for the CCIE Voice Written Exam Version 3.0



Email
sales@ccbootcamp.com

Phone
1.877.NLI.CCIE (654.2243)
Int'l: +1 702.968.5100

Website
www.ccbootcamp.com

Forums
www.routerie.com
www.securityie.com
www.voiceie.com



CCBOOTCAMP'S CCIE Voice Written Exam Study Guide

for the current CCIE Voice Written Exam

For questions about this workbook please visit: www.voiceie.com

CCBOOTCAMP

375 N. Stephanie Street
Building 21, Suite 2111
Henderson, NV 89014
1.877.654.2243 Toll Free

www.ccbootcamp.com

"Cisco," the "Cisco Logo," "CCNA," "CCNP," "CCDP," "CCDA," "CCIE," "Cisco Certified Network Associate," "Cisco Certified Design Professional," "Cisco Certified Design Associate," "and "Cisco Certified Network Professional," are registered trademarks of Cisco Systems, Inc. The contents contained wherein, is not associated or endorsed by Cisco Systems, Inc.

PLEASE READ THIS SUBSCRIPTION LICENSE AGREEMENT CAREFULLY BEFORE USING THIS PRODUCT. THIS SUBSCRIPTION LICENSE AGREEMENT APPLIES TO **CCBOOTCAMP's CCIE Voice Written Exam Study Guide**.

BY ORDERING THIS PRODUCT YOU ARE CONSENTING TO BE BOUND BY THIS LICENSING AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS LICENSE, THEN DO NOT PURCHASE THIS PRODUCT.

License Agreement

CCBOOTCAMP's CCIE Voice Written Exam Study Guide is copyrighted. In addition, this product is at all times the property of CCBOOTCAMP, and the customer shall agree to use this product only for themselves, the licensed user. The license for the specific customer remains valid from the purchase date until they pass their CCIE Voice written exam.

CCBOOTCAMP's CCIE Voice Written Exam Study Guide is licensed by individual customer. This material cannot be resold, transferred, traded, sold, or have the price shared in any way. Each specific individual customer must have a license to use this product. The customer agrees that this product is always the property of CCBOOTCAMP, and they are just purchasing a license to use it. A Customer's license will be revoked if they violate this licensing agreement in any way.

Copies of this material in any form or fashion are strictly prohibited. If for any reason a licensed copy of this material is lost or damaged a new copy will be provided free of charge, except for the cost of printing, shipping and handling.

Individuals or entities that knowingly violate the terms of this licensing agreement may be subject to punitive damages that CCBOOTCAMP could seek in civil court. Damages will be limited to a maximum of \$500,000.00 per individual and \$2,000,000.00 per entity. In addition, individuals or entities that knowingly violate the terms of this license agreement may be subject to criminal penalties as are allowed by law.

The venue of any dispute, controversy, litigation or proceeding (formal or informal) arising out of or pertaining to this licensing agreement or the subject hereof shall lie exclusively in the County of Clark, State of Nevada. Provided, however, that if any such dispute, controversy, litigation or proceeding requires or permits jurisdiction in a federal court or agency of the United States, then venue shall lie in no federal court or agency other than those located in (or nearest to) the County of Clark, State of Nevada.

Term and Termination of License Agreement

This License is effective until terminated. Customer may terminate this License at any time by destroying all copies of written and electronic material of said product. Customer's rights under this License will terminate immediately without notice from CCBOOTCAMP, if Customer fails to comply with any provision of this License. Upon termination, Customer must destroy all copies of material in its possession or control. The license for the specific user remains valid from the purchase date until the user passes their lab exam pertaining to the purchased subscription. Once the customer passes the relevant lab exam the license is terminated and all material written or electronic in their possession or control must be destroyed or returned to CCBOOTCAMP.

Warranty

No warranty of any kind is provided with this product. There are no guarantees that the use of this product will help a customer pass any exams, tests, or certifications, or enhance their knowledge in any way. The product is provided on an "AS IS" basis. In no event will CCBOOTCAMP, its suppliers, or licensed resellers be liable for any incurred costs, lost revenue, lost profit, lost data, or any other damages regardless of the theory of liability arising out of use or inability to use this product.

Study Guide for the Cisco CCIE Voice Written Exam

Author: Daryl P. Smith

Copyright© 2010 Network Learning, Inc.

Published by:

Network Learning Inc. (Cisco Learning Partner)

375 N. Stephanie Street, Building 21, Suite 2111

Henderson, NV 89014 USA

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system without written permission from the publisher except for the inclusion of brief quotations in a review.

Printed in the United States of America

Warning and Disclaimer

This book is designed to provide information to the Cisco CCIE Voice written exam. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The authors, editors, and Network Learning Inc., 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 book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Network Learning Inc.

Trademark Acknowledgements

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Network Learning Inc. cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Author – Daryl P. Smith

Daryl Smith is the author of CCBOOTCAMP's CCIE Voice Exam Strategy Guide Workbook. He has attained the highest level Cisco® certification: Cisco Certified Internetwork Expert: CCIE#25893 in Voice. Daryl is an experienced engineer with over 15 years in the networking and voice arena. Currently Daryl is working toward attaining his CCDE certification. He holds the following certifications: Cisco Certified Network Associate (CCNA), Cisco Certified Voice Professional (CCVP), Cisco Certified Internetwork Expert (CCIE-Voice#25893), and Cisco Certified System Instructor (CCSI) 33397.

Contributing Author – Brad Ellis

Brad Ellis (CCIE #5796, CCSI #30482, CSS1, CCDP, CCNP, MCNE, and MCSE) works as a network engineer and is the CEO of Network Learning Inc. He has been dedicated to the networking industry for over 12 years. Brad has worked on large scale security assessments and infrastructure projects. He is currently focusing his efforts in the security and voice fields. Brad is a dual CCIE (R&S / Security) #5796.

Contents

Contents	3
Introduction	27
Chapter 1 Infrastructure Protocols	28
DNS	28
Using DNS with CUCM Advantages	28
IP Address advantages	28
Cisco TFTP	29
TFTP Process Overview for SCCP Devices	30
TFTP Process Overview for Cisco Unified IP Phones Using SIP	31
Understanding How Devices Use DHCP and Cisco TFTP	32
Obtaining an IP Address	33
Requesting the Configuration File	33
Contacting Cisco Unified Communications Manager	34
NTP	35
SCCP Phones	36
SIP Phones	36
NTP for Network Devices	37
Power over Ethernet	37
Cisco AVVID and Cisco IP Communications	39
Inline Power	39

Cisco Inline Power	39
Statement of Direction	40
Voice and Data VLAN	41
Dynamic Host Configuration Protocol (DHCP)	41
Cisco IOS DHCP Server	41
Understanding Voice VLAN	42
Cisco IP Phone Voice Traffic	43
Cisco IP Phone Data Traffic	43
Default Voice VLAN Configuration	43
Single VLAN	44
Multi VLAN	44
Trunk Port VLAN	45
Troubleshooting Infrastructure Protocols	45
NTP	45
TFTP and DHCP	47
VLAN	48
Chapter 1 Questions	49
Chapter 1 Answers	52
Telephony Protocols	53
SCCP	53
Media Gateway Control Protocol (MGCP)	53

Call Connections for MGCP	56
PRI and BRI Backhaul	57
Configuring MGCP	58
Session Initiation Protocol (SIP)	58
SIP Entities	60
User Agent	61
Proxy Server	61
Redirect Server	61
Registrar	61
B2BUA	62
SIP Messages	62
SIP Request Messages	62
SIP Response Messages	62
SIP Addresses	63
Fully qualified domain names	63
E.164 addresses	63
Mixed addresses	63
Configuring SIP	64
SIP DTMF signaling	65
H.323	65
Terminals	67

Gateways	67
Gatekeepers	68
Multipoint Control Unit (MCU)	70
H.323 Version 2	71
Security	71
Fast Call Setup	71
Supplementary Services	71
T.120/H.323 Integration	72
H.323 Call Scenario	72
Basic H.323 Call Setup	72
Basic Configuration of an H.323 gateway	73
Call Flow with a Gatekeeper	74
Call Flow with multiple Gatekeepers	74
Configuring H.323	75
Strengths of H.323, SIP, and MGCP	77
H.323	77
SIP	77
MGCP	77
IP Voice Signal Interconnect CUBE	78
Requires one of these Cisco IOS feature sets:	79
Cisco Unified Border Element with Gatekeeper Network Topology	79

Real Time transport protocol (RTP)	82
Real Time Control Protocol - RTCP	83
Analog Interfaces	85
FXS	85
FXO	87
E&M	88
Digital Signaling (T1/E1)	90
CAS Systems: T1	90
Channel Associated Signaling	92
E1 Interface	92
CAS Systems: E1	93
E1 Channel Associated Signaling	94
Common Channel Signaling	94
CCS Signaling	94
ISDN	95
QSIG	96
ISDN PRI QSIG voice-signaling provides the following benefits:	96
IOS Dial-peer and Digit Manipulations	97
Dial Peer Overview	97
Call Legs	97
Destination Patterns	99

Types of Dial-Peers	99
Digit Manipulation	100
Wildcards	101
Digit Stripping and Prefixes	102
Forwarding Digits	104
Translation Rules	105
Features:	105
Assign Translation Profiles	105
voice translation-rule Command	107
Translation Profile Configuration	108
Dial Peer Configuration	108
Troubleshooting Telephony Protocols	108
MGCP	109
MGCP and H.323 controllers	110
ISDN debug	110
Active Calls on a Router	111
SIP	113
H.323 and Gatekeeper	115
Dial-peers	116
Call Control	118
Translation Rules	119

Chapter 2 Questions	120
Chapter 2 Answers	124
Chapter 3 Cisco Unified Communications Manager (CUCM)	125
Device Registration	125
Device Settings	126
Device Defaults Configuration	126
Phone Button Template	126
Softkey Templates	126
SIP Profile	127
Common Profile	127
Device Redundancy	128
Call Processing Redundancy	128
SRST-MGCP Fallback	129
Codec Selection	129
Dial Plan	130
Local Route Group	132
Support for + Dialing	134
Calling Party Number Transformations	136
Called Party Number Transformations	138
Globalize Call Routing Ingress and Egress	141
Constructing a Globalize Call Flow	144

Partitions	146
Calling Search Space	146
Digit Analysis	149
Digit collection	152
Type B SIP Phones	154
SIP Dial Rules	154
Digit Manipulation	156
Benefits of “+” Dialing	157
AAR	157
Call Forward Unregistered (CFUR)	158
Tail End Hop Off (TEHO)	158
Media Resources	158
Conference bridges	159
Media Termination Point	160
Annunciator	160
Transcoder	160
Cisco RSVP Agent	162
Music on Hold	162
Unicast and Multicast MoH	163
Cisco IP Voice Media Streaming Application	164
Media resource Manager (MRM)	165

Media Resource Group	165
Media Resource Group List	165
CUCM Applications	167
Extension Mobility (EM)	168
Unified CM Assistant	169
Unified CM Assistant Functionality and Architecture	170
Unified CM Assistant Share Lined Mode	171
Cisco Unified Mobility	172
Mobile Connect	173
Mobile Voice Access and Enterprise Feature Access	173
Remote Destination Profile Configuration	174
CUCM CTI Integrations	174
CTI Port	176
CTI Route Point	176
CUM Serviceability and OS Administration	177
Cisco OS Administration	177
CUCM Disaster Recovery	178
Troubleshooting CUCM	178
Dial Plan and Routing Issues	179
Route Partitions and Calling Search Spaces	180
Problem When Dialing a Number	182

Intercluster Cisco Unified IP Phone Calls	184
Intercluster H.323 Communication	185
Chapter 3 Questions	196
Chapter 3 Answers	207
Chapter 4 Cisco IOS IP Telephony	208
CUCME	208
CUCME Overview	208
SRST	209
Components of Centralized Call-Processing Architecture	210
When to user MGCP Fallback	212
When to Use Basic SRST:	212
When to Use CUCME SRST	213
SRST Timing	213
CUE	214
Deployment Models	215
Standalone Office	215
Multisite Networks	216
CUCME Call Features	217
Basic Automatic Call Distribution (B-ACD)	217
Customer Contact	218
IP Telephony	218

Rich-Media Conferencing	218
Third-Party Applications	218
Unified Communications	218
Video Telephony	219
IOS Media Resources	219
DSP Farms	219
DSP Farm Profiles	219
Conferencing	220
Transcoding	220
Media Termination Point	221
Allocation of DSP Resources Within the DSP Farm	222
Troubleshooting IOS Telephony	223
Telephony E-Phone & SIP Registration	223
Show ephone registered	224
Show voice register pool 1	224
Show telephony-service all & show voice register global	225
Chapter 4 Questions	227
Chapter 4 Answers	228
Chapter 5 - Quality of Service (QoS)	229
QoS Overview	230
Five Benefits for Implementing QoS in the Enterprise Networks	230

How a Converged Network Behaves Without QoS	231
QoS framework	231
Call Admission Control Functionality	231
Integrated Services vs. Differentiated Services	232
Configure QoS Policy using Modular QoS CLI	234
QoS Configuration overview	234
FIFO: default, no config necessary	234
CBWFQ:	235
CQ:	235
PQ:	235
LLQ:	236
CAR:	236
WRED:	237
FRED:	237
Link Fragmentation and Interleaving (LFI) for Multilink PPP (MLP):	238
Configure and Monitor Various LFI methods and CRTP	240
Classification and Marking	243
Purposes of Classification and Marking	243
Difference Between Classification and Marking	244
Class of Service, IP Precedence and DiffServ Code Points	244
Network Based Application Recognition (NBAR)	246

Classify and Mark Traffic	247
Congestion Management: Queuing	249
Identify and Differentiate Between IOS Queuing Techniques	250
Apply Each Queuing Technique to the Appropriate Application	253
IP RTP Priority and Low Latency Queuing (LLQ) Differences	254
Configure WFQ, CBWFQ, and LLQ	256
Congestion Avoidance	258
Explain How TCP Responds to Congestion	258
Explain Tail Drop and Global Synchronization	258
Identify and Differentiate Between: RED, WRED, FRED	259
Configure IOS Congestion Avoidance Features	260
Link Efficiency Tools	262
The Need for Link Efficiency Tools	262
Real Time Protocol Header Compression (cRTP)	264
Policing and Shaping	264
The Difference Between Policing and Shaping and How Each Relates to QoS	264
When to Apply and How to Configure Policing Mechanisms	265
Different Types of Traffic Shaping and How to Apply Them	265
Configure the Different Types of Traffic Shaping	267
Congestion-Control Mechanisms	269
Traffic Shaping Parameters	270

Traffic Shaping Calculation	270
First-In, First-Out (FIFO)	271
Weighted Fair Queuing (WFQ)	271
Priority Queuing	272
Custom Queuing	274
Class-Based Weighted Fair Queuing	276
Packet over SONET/SDH (PoS) and IP Precedence	277
IP Precedence	277
Random Early Detection (RED)	279
Weighted Random Early Detection (WRED)	279
Weighted Round-Robin (WRR)/Queue Scheduling	280
Class of Service (CoS)	281
Shaping vs. Policing	282
Traffic Shaping	282
Committed Access Rate (CAR)	285
Network-Based Application Recognition (NBAR)	286
Configuring NBAR	287
Differentiated Services Code Point (DSCP)	288
Resource Reservation Protocol (RSVP)	290
Load Balancing	291
802.1x and QoS	292

LAN QoS	310
Trust boundary	311
Connecting an IP Phone	312
AutoQoS	313
AutoQoS VoIP	314
AutoQoS Enterprise	315
3750 QoS	315
Default Ingress QoS Configuration	316
Congestion Management and Avoidance	317
Queueing and Scheduling	318
Egress QoS Features	319
Default Configuration	320
Chapter 5 Questions	322
Chapter 5 Answers	331
Chapter 6 – Unified Messaging	332
Integration	332
Integration Capabilities	334
Integration Functionality SCCP & SIP	336
Digital Integration with Digital PIMG Units	338
DTMF Integration with Analog PIMG Units	339
Serial (SMDI, MCI, or MD-110) Integration with Analog PIMG Units	340

Call Information	341
Integration Functionality	341
Integration Description TIMG	342
Serial Integration with TIMG Units	342
In-Band Integration with TIMG Units	343
Call Information	344
Integration Functionality	344
Deployment Models	345
Single-Site Messaging	345
Centralized Messaging	346
Distributed Messaging	347
MWI	348
MWI Format	349
SMDI integration	349
The forwarded call format is:	351
Call Handlers	352
Directory Handlers	353
Default System Call Handlers	354
Overview of Call Handler Greetings	355
Standard Greeting for Call Handlers	356
Offering One-Key Dialing During Call Handler Greetings	357

Offering System Transfers	358
Abbreviated Extensions: Prepending Digits to Extensions That Callers Enter	358
Taking Messages	359
Transferring Calls	359
Directory Call Handlers	361
Creating a Directory Handler	361
Interview Handlers	362
VPIM	362
Interoperability with disparate systems:	363
VPIM Concepts	363
The following VPIM concepts will be explained:	363
VPIM Messages	363
VPIM Addresses	365
Messaging Similarities and Limitations	366
Audio Format Considerations	367
Troubleshooting Unified Messaging	368
Unity Connection Traces	368
Traces with Cisco Unity Express	368
MWIs Do Not Turn On or Off	369
Task List for Troubleshooting When MWIs Do Not Turn On or Off:	369
Utilities	370

Cisco Unity Connection Grammar Statistics Tool	370
Cisco Unity Connection Serviceability	371
Cisco Unity Connection Task Management Tool	372
Cisco Voice Technology Group Subscription Tool	372
Real-Time Monitoring Tool	372
Cisco Unified Serviceability	373
Remote Database Administration Tools	374
Cisco Utilities Database Link for Informix (CUDLI)	374
Remote Port Status Monitor	374
Chapter 6 Questions	375
Chapter 6 Answers	377
Chapter 7 Integration	378
IPCC overview	378
Deployment Models	379
IPCC Express co-resident	380
Single-Server Non-HA Deployment Model	380
Multi-Server Non-HA Deployment Model	381
Two-Server HA Deployment Model	382
Four-Server HA Deployment Model	383
Six-Server HA Deployment Model	384
Ten-Server HA Deployment Model	385

User Accounts	386
CTI Ports	386
CTI Route Points	387
Accessing Cisco Unified CCX Administration	387
Cisco Unified Communications Manager Configuration Page	388
Resource Manager-Contact Manager	388
Control Center	389
Prompt Management	390
Script Management	391
Resource Manager-Contact Manager	393
Scripting	393
Basic Script	402
Select Resource	403
Connect Step	404
Call Hold/ Call Unhold	404
Get Reporting Statistic	404
Troubleshooting Cisco Unified CCX	406
Troubleshooting Tips	406
Debugging a Script	408
Reactive or Non-Reactive Debugging	409
Trace Log Files	410

Alarm Configuration	411
Chapter 7 Questions	413
Chapter 7 Answers	417
Chapter 8 – Presence	418
Presence Components	418
The Message Flow, Publish, and Subscribe	421
CUPS Administration	423
CUPC – Cisco Unified Personal Communicator	423
Cisco Unified Presence – Settings.	432
Users not showing up in CUPS user list	436
Troubleshooting using the Cisco Unified Personal Communicator	437
Server Health Tool	437
Audio and Video	438
Questions Chapter 8	439
Answers Chapter 8	442
Chapter 9 - UC Security	443
Security Overview	443
DHCP Snooping	444
Phone Authentication and Encryption	445
Disabling the Gratuitous ARP Setting	446
Disabling Web Access Setting	446

Disabling the PC Voice VLAN Access Setting	447
Disabling the Setting Access Setting	447
Disabling the PC Port Setting	448
PKI Topologies in CUCM Deployments	448
Initial Download of the CTL	453
IP Phone Usage of the CTL	453
Firewalls, Gateway Security & NAT	454
Overview for Cisco IOS MGCP Gateway Encryption	454
Overview for SIP Trunk Encryption	455
NAT	456
Implementing Firewall Traversal and NAT	456
TCP/UDP Port List	457
Chapter 9 Questions	460
Chapter 9 Answers	463
Chapter 10 - Application Protocols	464
IP Multicast	464
Benefits of IP Multicast	464
IGMP and CGMP Multicast Protocols	465
Designated Querier	467
Querier router election	467
IGMP Versions 1, 2, and 3	468

Multicast Address Allocation	470
Static Address Allocation Methods	470
Scope Relative Address Allocation	470
Dynamic Address Allocation	471
SDR—Session Directory	471
Classic PIM-SM	471
Bidirectional PIM	472
IP Multicast Routing	473
Multicast Groups	473
Rendezvous Points (Auto-RP, BSR)	475
Recommended Rendezvous Point Placement	476
Group-RP Mapping Mechanism	476
Recommendation	476
Comments on Auto-RP	477
Comments on Static RP	478
Calculating a Multicast Address	478
Protocol Independent Multicast (PIM)	479
PIM Commands	481
Reverse Path Forwarding (RPF)	481
PIM and Distance Vector Multicast Routing Protocol (DVMRP)	481
PIM-SM Mechanics (Joining, Pruning PIM State, Mroute table)	482

PIM-SM uses these PIMv2 messages	482
PIM-DM	483
Bidirectional PIM (bidir-PIM)	484
Designated Forwarder (DF) Election	486
Bidirectional Group Tree Building	487
Packet Forwarding	488
Memory, Bandwidth, and CPU Requirements	488
Benefits and Drawbacks of PIM	489
Debugging bidir-PIM is easier than PIM-SM	489
RP Tree Delivery for All Packets	489
Bidir-PIM Partial Upgrades Not Allowed	489
Bidir-PIM Network Redundancy Not Supported	490
Bidir-PIM Nonbroadcast Multi-access Mode Not Supported	490
Bidir-PIM Traffic Forwarding Restrictions	490
Anycast RP	492
IP Multicast Terms	492
Unicast & Multicast for CUCM/CUCME	497
Video	499
Video Codec	499
Video Call Bandwidth	500
Cisco Video Telephony Advantage (CVTA)	501

Fax and Modem	502
Overview of Fax and Fax Relay	502
Fax Relay Basics	503
Chapter 10 Questions	506
Chapter 10 Answers	509
Chapter 11 Operation and Network Management	510
Operating System Status and Configuration	510
Settings	510
Software Upgrades	511
UC Product Upgrade	511
Traces	512

Introduction

This book is targeted toward the potential Cisco CCIE Voice candidates preparing for the new CCIE Voice Exam based upon Cisco Unified Communications Manager 7.0, Unity Connection 7.0, Cisco Unified Presence Server and Cisco Unified Contact Center Express. The written guide is more than just a guide to assist you in passing the written exam (350-030), but to assist you with your career as well. This guide can also be used as a reference guide for it contains a combination of notes, white papers and Cisco technical tutorial as well classroom material from CCBOOTCAMP.

This guide also provides some sample questions that are not directly related to actual questions you will see on the exam but questions that will help you understand the topics and concepts within each chapter. These questions serve as a guide and will help you build confidence as you prepare for the CCIE Voice Written Exam. Some of the concepts are complex and this guide will help you understand these concepts as you prepare for the written exam as well as the CCIE Voice Lab exam.

I also recommend you read the CUCM SRND guide found on www.cisco.com/go/srnd and additional material found on Cisco Learning Network for CCIE candidate: https://learningnetwork.cisco.com/community/certifications/ccie_voice

This is your first step in a long journey to becoming a CCIE. This journey is not an easy one but it is one that you will enjoy once you succeed. Once you obtain your CCIE you will be recognized as one of the elites in the industry, for you have demonstrated your knowledge and capability to perform complex concepts. Good luck in your journey and remember to enjoy it.

Daryl P. Smith, September 2010

Chapter 1 Infrastructure Protocols

DNS

DNS within Cisco Unified Communications Manager clusters has some advantages and disadvantages. DNS is used to for name resolution and it allows CUCM services and applications to reference the server/system by name instead of by IP address.

Cisco Unified Communications Manager can use either IP addresses or host names to refer to other devices such as server or application settings within the cluster. When host names are used, the CUCM server must be able to resolve the names. Therefore; a DNS server is required within the environment.

Using DNS with CUCM Advantages

In the case of using DNS, management is simplified because logical names are simpler to handle than 32-bit addresses. If IP addresses change, there is no need to modify the application settings, because they can still use the same names; only the DNS server configuration needs to be modified in this case. IP addresses of CUCM server can be translated by NAT toward IP Phones, because the IP phone configuration files do not include the original server IP address. When the DNS requests are sent out by IP Phones, the use of NAT for the server IP addresses is no problem, for the phones are using a hostname and not the IP address.

IP Address advantages

The system doesn't depend on DNS for name resolution. A device (IP Phone) can initiate a request directly to the target and the time required for an established connection is reduced. By eliminating the need for DNS, there are no errors caused by DNS misconfiguration. Troubleshooting is simplified because there is no need to verify proper name resolution.

Best Practice recommendation is not use DNS with Cisco Unified Communications Manager.

If DNS is used within the environment, there are some components that will require DNS and rely on the availability of the DNS server or servers.

IP Phones will require DNS for signaling when CUCM servers are configured by names. The configured CUCM server is part of the configuration file of the IP Phone. Therefore an IP Phone needs to be able to resolve the name of the CUCM server or servers to an IP address when CUCM server is specified by name. By default CUCM servers are added to the configuration database by their name. IP Phones also need to be capable of resolving names of IP Addresses when IP Phone service URLs use names instead of IP addresses. This applies to service accessed from the services button at the phone, and to services that are accessed by phone buttons configured with service URLs.

SIP Trunks, SIP Gateways, H.323 Gateways and H.323 Trunks can be configured to use Host Names as well as SIP route patterns and SNMP and other network management servers.

Cisco Unified Communications Manager servers never use DNS for intracluster communications; Cisco Unified Communications Manager servers always use IP addresses, regardless of whether host names are configured for the servers.

Cisco TFTP

The Cisco TFTP service builds and serves files that are consistent with the Trivial File Transfer Protocol (TFTP). Cisco TFTP builds configuration files and serves embedded component executables, ringer files, and device configuration files. A configuration file contains a prioritized list of Cisco Unified Communications Managers for a device (phones that are running SCCP and phones that are running SIP and gateways), the TCP ports on which the device connects to those Cisco Unified Communications Managers, and an executable load identifier. Configuration files for selected devices contain locale information and URLs for the phone buttons: messages, directories, services, and information. Configuration files for gateways contain all their configuration information. You can find configuration files in a .cnf, a .cnf.xml, or an .xml format, depending on the device type and your TFTP service parameter settings. When you set the BuildCNFType service parameter to

Build All, the TFTP server builds both .cnf.xml and .cnf format configuration files for all devices. When you set this service parameter to Build None, the TFTP server builds only .cnf.xml files for all devices. When this parameter is set to Build Selective, which is the default value, the TFTP server builds .cnf.xml files for all devices and, in addition, builds .cnf files only for a select list of device types.

TFTP Process Overview for SCCP Devices

The TFTP server can handle simultaneous requests for configuration files. The request process is as follows: When a device boots, it queries a DHCP server for its network configuration information. The DHCP server responds with an IP address for the device, a subnet mask, a default gateway, a Domain Name System (DNS) server address, and a TFTP server name or address. Cisco Unified IP Phone 796X, for example, supports up to two TFTP servers. If the primary TFTP server is not reached, such devices attempt to reach the fallback TFTP server. The device requests a configuration file from the TFTP server. The TFTP server searches three internal caches, the disk, and then alternate Cisco file servers (if specified) for the configuration file. If the TFTP server finds the configuration file, it sends it to the device. If the configuration file provides Cisco Unified Communications Manager names, the device resolves the name by using DNS and opens a connection to the Cisco Unified Communications Manager. If the device does not receive an IP address or name, it uses the TFTP server name or IP address for setting up its registration connection. If the TFTP server cannot find the configuration file, it sends a message to the device.

"file not found"

Devices that are requesting a configuration file while the TFTP server is rebuilding configuration files or while processing the maximum number of requests, receive a message from the TFTP server, which causes the device to request the configuration file later. The Maximum Serving Count service parameter, which can be configured, specifies 200 as the maximum number of requests.

TFTP Process Overview for Cisco Unified IP Phones Using SIP

Unlike phones that are running SCCP, phones that are running SIP get all their configurations from the TFTP server. From initial startup, the phone that is running SIP contacts the configured TFTP server (either manually configured or configured through the DHCP server) to get the configuration files; it then registers itself to its configured Cisco Unified Communications Manager.

When the configuration of the phone that is running SIP gets changed, the Cisco Unified Communications Manager database notifies the TFTP server to rebuild all the configuration files or to rebuild selectively. The TFTP server retrieves information from the Cisco Unified Communications Manager database and converts it into the proper output format, according to the device type, and saves the output in TFTP cache. When the TFTP server gets a request, it searches either the cache or Alternate File Server locations disk to serve the requested configuration file or default files.

The TFTP support for phones that are running SIP builds and serves different formats of SIP configuration files from the Cisco Unified Communications Manager database for the following Cisco Unified IP Phones:

- Cisco Unified IP Phone 7970/71, 7961, 7941, 7911 (These phones share the same SIP configuration file format).
- Cisco Unified IP Phone 7960, 7940 (These phones share the same SIP configuration file format).
- Cisco Unified IP Phone 7905, 7912
- SIP dial plans on the preceding phones
- Softkey templates on the preceding phones

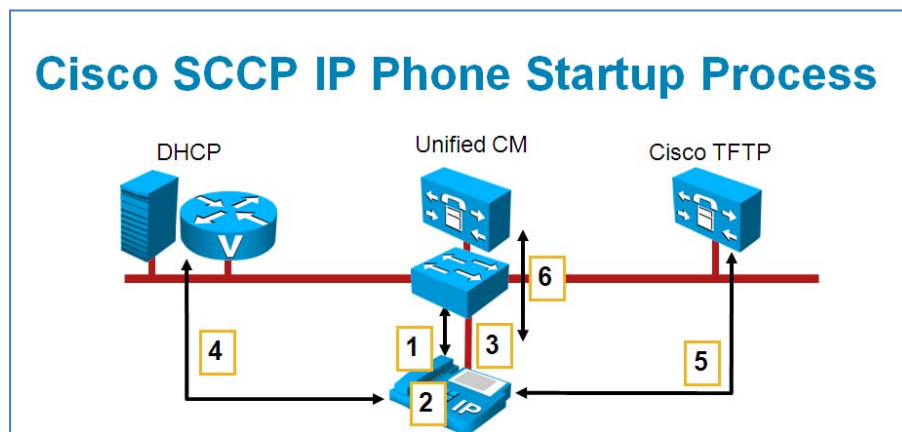
The TFTP server generates the following files from the Cisco Unified Communications Manager database for configuration of phones that are running SIP:

- System wide default configuration files and per-device configuration files.

- List of system wide dial plans for Cisco Unified IP Phones 7970/71, 7960/61, 7940/41, and 7911.
- List of system wide softkey template files.

The system derives filenames from the MAC Address and Description fields in the Phone Configuration window of Cisco Unified Communications Manager Administration and the device name field in the Cisco Unified Communications Manager database. The MAC address uniquely identifies the phone.

Understanding How Devices Use DHCP and Cisco TFTP



1. Cisco IP phone obtains power from the switch
2. Cisco IP phone loads locally stored image
3. Switch provides VLAN information to Cisco IP phone using Cisco Discovery Protocol
4. Phone sends DHCP request; receives IP information and TFTP server address
5. Cisco IP phone gets configuration from TFTP server
6. Cisco IP phone registers with Cisco Unified Communications Manager server, Unified CM sends softkey template to SCCP phone using SCCP messages.

Cisco telephony devices require IP addresses that are assigned manually or by using DHCP. Devices also require access to a TFTP server that contains device loads and device configuration files.

Obtaining an IP Address

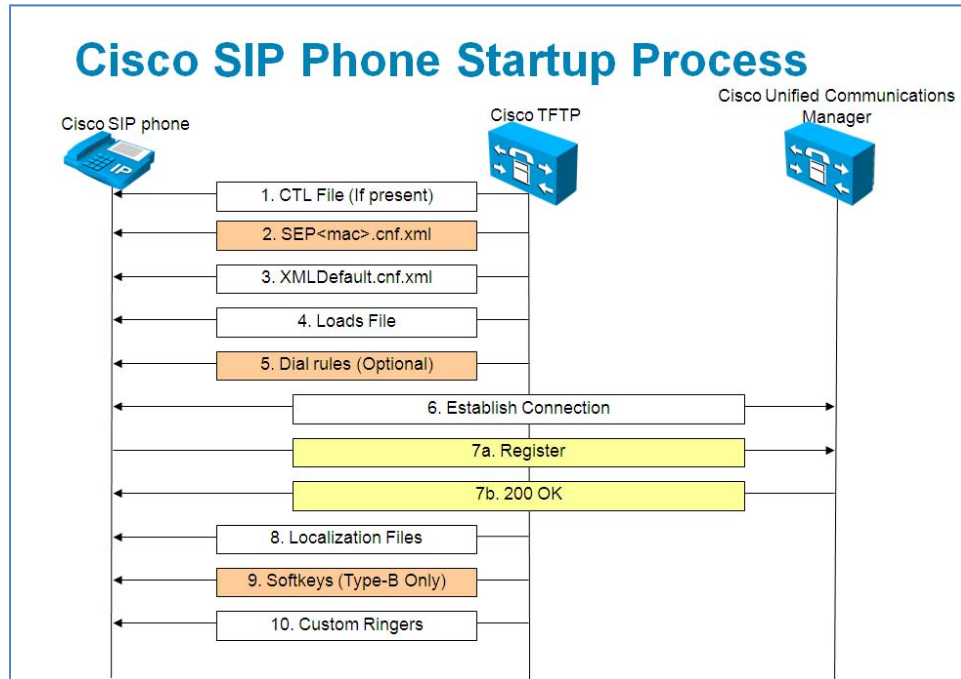
If DHCP is enabled on a device, DHCP automatically assigns IP addresses to the device when you connect it to the network. The DHCP server directs the device to a TFTP server (or to a second TFTP server, if available for the device). For example, you can connect multiple Cisco Unified IP Phones anywhere on the IP network, and DHCP automatically assigns IP addresses to them and provides them with the path to the appropriate TFTP server. If DHCP is not enabled on a device, you must assign it an IP address and configure the TFTP server locally on the device.

The default DHCP setting varies depending on the device:

- Cisco Unified IP Phones stay DHCP-enabled by default. If you are not using DHCP, you need to disable DHCP on the phone and manually assign it an IP address.
- DHCP always remains enabled for Cisco Access Analog and Cisco Access Digital Gateways.

Requesting the Configuration File

After a device obtains an IP address (through DHCP or manual assignment), it requests a configuration file from the TFTP server. If a device has been manually added into the Cisco Unified Communications Manager database, the device accesses a configuration file that corresponds to its device name. If a phone is not manually configured and auto-registration is enabled, the phone requests a default configuration file from the TFTP server and starts the auto-registration procedure with Cisco Unified Communications Manager. If a phone has an XML-compatible load, it requests a .cnf.xml format configuration file; otherwise, it requests a .cnf file.



Contacting Cisco Unified Communications Manager

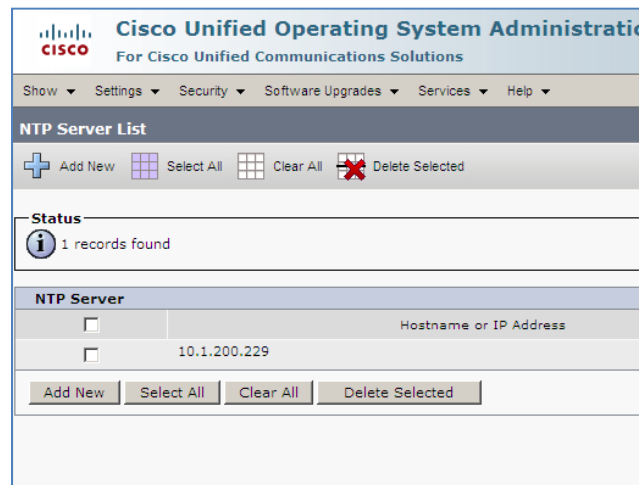
After obtaining the configuration file from the TFTP server, a device attempts to make a TCP connection to the highest priority Cisco Unified Communications Manager in the list that is specified in the configuration file. If the device was manually added to the database, Cisco Unified Communications Manager identifies the device. If auto-registration is enabled in Cisco Unified Communications Manager, phones that were not manually added to the database, attempt to auto-register in the Cisco Unified Communications Manager database. Cisco Unified Communications Manager informs devices that are using .cnf format configuration files of their load ID. Devices that are using .xml format configuration files receive the load ID in the configuration file. If the device load ID differs from the load ID that is currently executing on the device, the device requests the load that is associated with the new load ID from the TFTP server and resets itself. A phone gets the Ring Tones list after it performs its booting process, when the user wants to modify the Default Phone Ring setting, and when the user loads new ring tones.

NTP

Date and Time are important for devices within a Cisco Unified Communications Cluster and all of the applications servers used as well; Cisco Unity Connection, Cisco Unified Presence, etc. Network devices as well as servers may require time synchronization and replication of data within a database cluster to have specific time stamps.

Network Time Protocol (NTP) is a protocol for synchronizing the clocks of systems within an IP network. NTP has a hierarchical organization using clock strata. Stratum 0 is an extremely precise clock source, such as an atomic clock or a radio clock. A stratum 1 server is directly connected to a stratum 0 clock and can provide time information to other devices, which themselves can serve stratum 3 devices.

The use of NTP on all devices ensures that they all have synchronized clocks. The Publisher sends NTP request to an external NTP server and the subscribers always synchronize their time with the publisher. The configuration of an external NTP server is not mandatory. If no NTP server is configured, the publisher relies on its own system time. NTP can be enabled and configured during installation or after installation. To configure NTP after installation you make the changes with Cisco Unified Communication Manager OS Administration. Settings-> NTP Servers.



System time is important within CUCM cluster. The following items depend upon an accurate clock being set and synchronized:

- Cisco IP Phone display date and time information
- Call Detail Records and Call Management Record (CDR and CMR)
- Alarms and event logs and Trace Files information for Troubleshooting
- Some Cisco Unified Communications Manager Features are date or time-based and therefore rely on having the correct date and time. Time-of-day routing and certificate-based security features

To ensure that all network devices have the correct date and time it is recommended that all network devices use NTP for time synchronization. The master reference clock should be a stratum 1 NTP server.

SCCP Phones

SCCP phones obtain date and time information from the Cisco Unified Communications Manager. The Date/Time Group value, which is configured at the phones device pool, is considered to allow phones deployed at different time zones to display the local time only, not sync their time.

SIP Phones

SIP phones on the other hand must obtain their time from one or more configured NTP references. These references are added to the Date/Time group and are therefore applied to the phone via the device pool. The NTP reference is applicable only to SIP phones. If a SIP Phone doesn't have a NTP reference configured, or none of the configured servers are reachable, the SIP phone obtains time information from the SIP signaling message received from CUCM. It extracts the time from the time stamp of the 200 OK messages it receives.

NTP for Network Devices

For network devices with a Cisco Unified Communications cluster, IOS devices can act as NTP servers or clients. They can transmit either unicast or broadcast messages to server or clients.

The Cisco IOS implementation of NTP supports additional features such as authentication and access restrictions. If a Cisco IOS device is configured as an NTP server, it can be used as an external NTP server by the CUCM publisher. As stated in the previous section for CUCM NTP, subscribers always synchronize their time from the publisher. An external NTP server can be configured only at the publisher server, not on any other nodes within the cluster.

To configure an IOS device as a NTP server, the following commands must be entered on the device.

```
Router (config) #ntp master 2
! configures router as an NTP source
Router (config)#ntp source loopback 0
! configures source interface for NTP
Router (config)#ntp server 10.1.200.229
! specifies the NTP Server
```

You should always configure your Cisco IOS devices within your environment with a NTP reference. Also you should configure summer time range and date and time stamps for debugging and logging.

Power over Ethernet

Power over Ethernet (PoE) allows the LAN switching infrastructure to provide power to an endpoint ("powered device") over a copper Ethernet cable. This capability, once referred to as "inline power," was originally developed by Cisco in 2000 to support emerging IP telephony deployments.

IP telephones need power for operation, and Power over Ethernet supports scalable, manageable power delivery and simplifies IP telephony deployments. As wireless