Application Note

Telnet SIP Trunking: Connecting Cisco Unified Communications Manager 8.6(1) via the Cisco Unified Border Element 8.6 using SIP

February 25, 2012

Table of Contents

Note: Testing was conducted in *tekVizion* labs.

Introduction

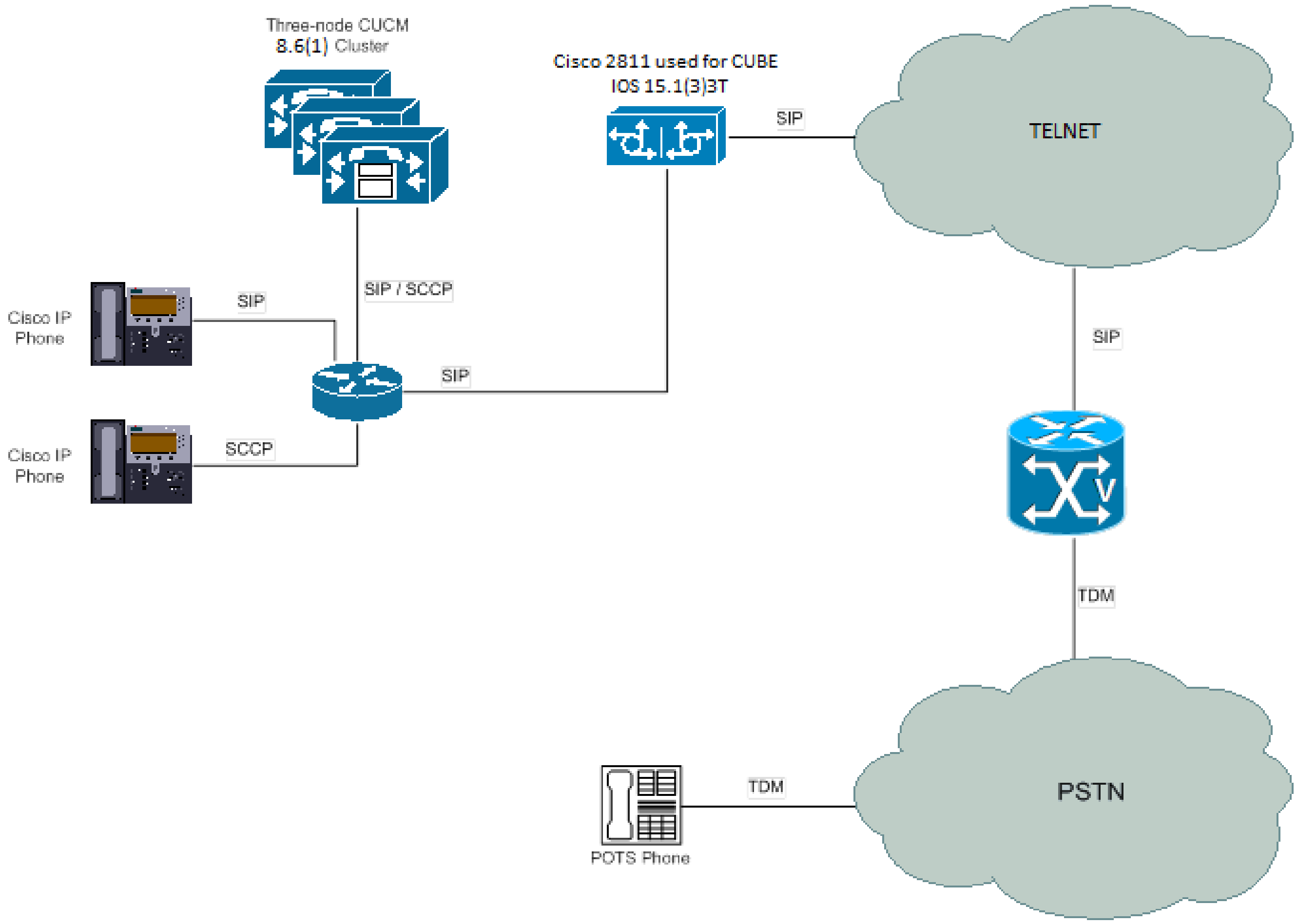
Service Providers today, such as Telnet, are offering alternative methods to connect to the PSTN via their IP network. Most of these services utilize SIP as the primary signaling method and a centralized IP to TDM gateway to provide on-net and off-net services. Telnet SIP Trunking is a service provider offering that allows connection to the PSTN and may offer the end customer a viable alternative to traditional PSTN connectivity via either Analog or T1 lines. A demarcation device between these services and customer owned services is recommended. The Cisco Unified Border Element provides demarcation, security, interworking and session management services.

- This application note describes how to configure a Cisco Unified Communications Manager (Cisco UCM) 8.6(1) with a Cisco Unified Border Element (Cisco UBE) for connectivity to the Telnet® SIP Trunking service. The deployment model covered in this application note is CPE (Cisco UCM 8.6(1)/Cisco UBE) to PSTN via Telnet® SIP Trunking. This document does not address 911 emergency outbound calls. For 911 feature service details contact Telnet , directly.
- Testing was performed in accordance to Cisco's Service Provider SIP Trunk Validation Test Plan and all features were verified. Key features verified are:
  - Basic Calls
  - Basic Calls with Calling Name and Number as allowed or restricted
  - DTMF Relay
  - Call Conference (Intra-site, PSTN)
  - Call Transfer (Blind, Attended, Early Attended)
  - Hold and Resume
  - Voice Mail
  - T.38 Fax G3/SG3
  - Simultaneous Calls
  - Auto Attendant
  - International Calls
  - G.711 Fax G3/SG3
  - Call Forwarding – Find Me (Unconditional, Busy, No Reply)
  - Codec negotiation
  - Dial Plans
  - PRACK with SDP early-media cut-through
- The Cisco Unified Border Element configuration detailed in this document is based on a lab environment with a simple dial-plan used to ensure proper interoperability between Telnet SIP network and Cisco Unified Communications. The configuration described in this document details the important commands to have enabled for interoperability to be successful and care must be taken, by the network administrator deploying Cisco UBE, to ensure these commands are set per each dial-peer requiring to interoperate to Telnet SIP network.
- This application note does not cover the use of calling search spaces (CSS) or partitions on Cisco Unified Communications Manager. To understand and learn how to apply CSS and partitions refer to the cisco.com link below:
  http://www.cisco.com/en/US/partner/docs/voice_ip_comm/cucm/admin/8_0_2/ccmsys/a03ptcss.html

Note: Testing was conducted at tekVizion Labs®.

Network Topology

Figure 1. Lab Network Topology



System Components

Hardware Components

- Cisco 2811
- Cisco Unified Communications Manager (1-node cluster consisting of Cisco MCS 7800 Series servers)
- Cisco IP Phones
- TELNET - - GenBand C3 MGC
- TELNET - - GenBand G9 MG
- TELNET - - GenBand S3 SBC
- TELNET - - BroadSoft/BroadWorks

Note: Testing was conducted at tekVizion Labs®.

Software Requirements

- Cisco Unified Communications Manager 8.6.1.20000-1
- Cisco Unified Border Element, IOS version 15.1(3)3T (C2800NM-SPSERVICESK9-M)
- TELNET - - GenBand C3 MGC Rel. 8.1.58.05
- TELNET - - GenBand G9 MG Rel. 0801.05.03
- TELNET - - GenBand S3 SBC Rel. 7.1.6.8
- TELNET - - BroadSoft/BroadWorks Rel. 17.4

Note: Testing was conducted at tekVizion Labs®.

Features

Features Supported

- Voice calls using G.729 and G.711 codecs
- RFC 3261 support
- Calling number presentation / restriction
- Call conferencing
- Call transfer (attended and unattended)
- Call hold and resume
- Call forwarding
- DTMF relay (RFC 2833)
- Early media cut-through with DTMF relay before 200 OK
- G.711 pass-through fax

Features Not Supported

- Caller ID update via SIP UDATE method
- T.38 fax

Note: Testing was conducted at tekVizion Labs®.

Caveats

- Special consideration is required with the FROM header. Telnet only accepts INVITE requests with a FROM header that has a TelnetID. If caller id presentation is required, the information must be included in the P-asserted-identity, and synchronized with information provisioned on Telnet portal.
- Special consideration is required with the URI header on incoming call from Telnet. The Telnet network always send the pilot number registration on the request URI header and destination number in the TO header . CUCM use the URI header to route the call and not the TO header. The INVITE and CANCEL message require header manipulation that copy the TO header user part (Called number) to the URI header.
- When a PSTN to CPE call is transferred by the CPE to a second PSTN number, the Caller ID displayed on the transfer target is the CPE DID number. Telnet does not update to the original PSTN calling party number when the transfer is completed. Telnet does not support the UPDATE method.

Note: Testing was conducted at tekVizion Labs®.

Call Flows

In the sample configuration presented here, CUCM is provisioned with four-digit directory numbers. And the last 4 digits corresponding to the Extension.

For incoming PSTN calls, the CUBE presents the full ten-digit DID number to CUCM. The CUCM trunk configuration strips all but the last four digits. Voice calls are routed to IP phones;

CPE callers make outbound PSTN calls by dialing a "91" prefix followed by the destination number. A "91.@" route pattern strips the prefix and routes the call with the remaining digits via a SIP trunk terminating on the CUBE.

Figure 2. Outbound Voice Call

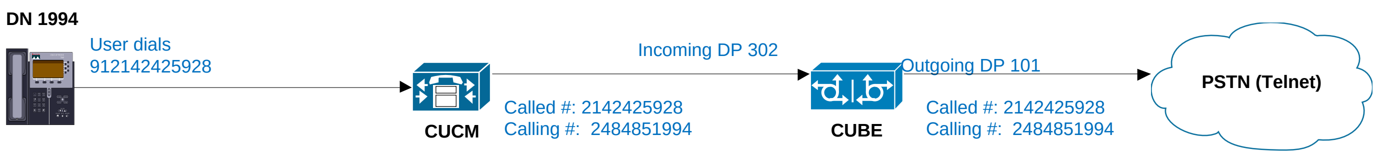
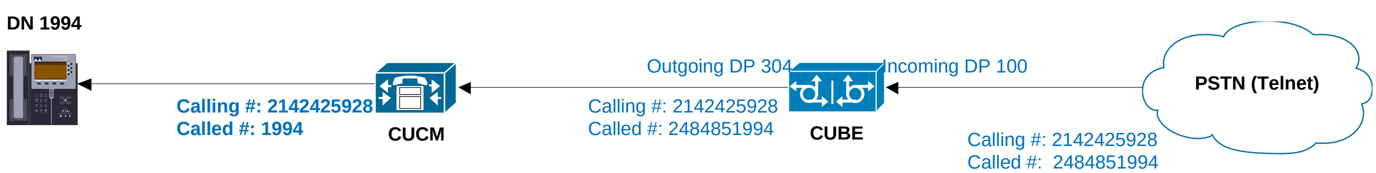


Figure 3. Inbound Voice Call



Note: Testing was conducted at tekVizion Labs®.

Configuration

Configuring Cisco Unified Border Element

Critical commands are marked in **Bold** with footnotes at the bottom of the page

Version Information:

```
Cisco IOS Software, 2800 Software (C2800NM-SPSERVICESK9-M), Version 15.1(3)T3, RELEASE SOFTWARE (fc1)

Technical Support: http://www.cisco.com/techsupport

Copyright (c) 1986-2011 by Cisco Systems, Inc.

Compiled Wed 14-Dec-11 21:01 by prod_rel_team


ROM: System Bootstrap, Version 12.4(13r)T5, RELEASE SOFTWARE (fc1)


Main2811 uptime is 5 days, 52 minutes

System returned to ROM by reload at 15:16:04 CST Fri Jan 27 2012

System restarted at 15:19:22 CST Fri Jan 27 2012

System image file is "usbflash0:c2800nm-spservicesk9-mz.151-3.T3.bin"

Last reload type: Normal Reload



This product contains cryptographic features and is subject to United

States and local country laws governing import, export, transfer and

use. Delivery of Cisco cryptographic products does not imply

third-party authority to import, export, distribute or use encryption.

Importers, exporters, distributors and users are responsible for

compliance with U.S. and local country laws. By using this product you
```


Note: Testing was conducted at tekVizion Labs®.

```
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco 2811 (revision 53.51) with 247808K/14336K bytes of memory.
Processor board ID FHK0923F0YT
2 FastEthernet interfaces
25 Serial interfaces
1 Channelized T1/PRI port
DRAM configuration is 64 bits wide with parity enabled.
239K bytes of non-volatile configuration memory.
976880K bytes of USB Flash usbflash0 (Read/Write)
62720K bytes of ATA CompactFlash (Read/Write)
```

Running Configuration:

```
Current configuration : 7015 bytes
!
! Last configuration change at 15:41:08 CST Wed Feb 1 2012 by cisco
! NVRAM config last updated at 16:09:01 CST Tue Jan 31 2012 by cisco
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Main2811
!
boot-start-marker
boot system usbflash0:c2800nm-spservicesk9-mz.151-3.T3.bin
boot-end-marker
```


Note: Testing was conducted at tekVizion Labs®.

```
!
card type t1 1 0
logging buffered 51200 warnings
no logging console
enable secret 5 $1$ELsJ$rMOpADTplX/DtwNNBHvhY0
!
aaa new-model
!
aaa session-id common
clock timezone CST -6 0
clock summer-time CDT recurring
no network-clock-participate slot 1
!
voice-card 0
!
voice-card 1
 dspfarm
 dsp services dspfarm
!
dot11 syslog
ip source-route
!
ip cef
!
ip domain name lab.tekvizion.com[1]
ip name-server 10.64.1.3[2]
no ipv6 cef
ntp server 10.10.10.5
multilink bundle-name authenticated
!
isdn switch-type primary-ni
!
voice rtp send-recv
!
voice service voip
ip address trusted list[3]
  ipv4 0.0.0.0 0.0.0.0
 allow-connections sip to sip[4]
 fax protocol t38 version 0 ls-redundancy 0 hs-redundancy 0 fallback none[5]
sip
  rel1xx disable
  asserted-id pai
  early-offer forced[6]
  midcall-signaling passthru

!
voice class uri TRUNK sip
 user-id 248485199.
voice class codec 1
 codec preference 1 g729r8
 codec preference 2 g711ulaw
```

[1] Optional, for use with a multiple-subscriber cluster. The domain name must match the CUCM enterprise parameter "Cluster Fully Qualified Domain Name" and must resolve to a DNS SRV. See "DNS Configuration" and "CUCM Configuration" below.

[2] IP address of DNS server
[3] IP address trusted list allowed to CUBE, only allow the network configure in this list.
[4] Allow SIP to SIP call processing
[5] Fax configuration for T38, to use G711u pass through change this line to: fax protocol pass-through g711ulaw
[6] Configures CUBE to send a SIP INVITE with SDP on an outbound call leg (Delayed Offer to Early Offer)

Note: Testing was conducted at tekVizion Labs®.

```
voice class sip-profiles 1[7]
 request INVITE peer-header sip TO copy "sip:(.*)@" u01
 request CANCEL peer-header sip TO copy "sip:(.*)@" u02
 request INVITE sip-header SIP-Req-URI modify ".*@(.*)" "INVITE sip:\u01@\1"
 request INVITE sip-header To modify ".*@(.*)" "To: <sip:\u01@\1"
 request CANCEL sip-header SIP-Req-URI modify ".*@(.*)" "CANCEL sip:\u02@\1"
 request CANCEL sip-header To modify ".*@(.*)" "To: <sip:\u02@\1"
!
voice class sip-profiles 2[8]
 request INVITE sip-header P-Asserted-Identity modify "174.46.0.150" "asmain.voip.telnetww.com"
 response ANY sdp-header Audio-Attribute modify "sendonly" "sendrecv"
 request ANY sdp-header Audio-Attribute modify "sendonly" "sendrecv"
!
voice class sip-copylist 1
 sip-header TO
!
crypto pki token default removal timeout 0
!
license udi pid CISCO2811 sn FHK0923F0YT
archive
 log config
  hidekeys
username cisco password 0 cisco
!
controller T1 1/0/0
 cablelength long 0db
 pri-group timeslots 1-24
!
interface FastEthernet0/0
 description Internal LAN (CUCM-facing)
 ip address 10.64.1.88 255.255.0.0
 duplex full
 speed 100
!
interface FastEthernet0/1
 description External WAN (Service Provider facing)
 ip address 174.46.0.150 255.255.255.128
 duplex full
 speed 100
!
interface Serial0/0/0
 no ip address
 shutdown
!
interface Serial1/0/0:23
 no ip address
 encapsulation hdlc
 isdn switch-type primary-ni
 isdn timer T310 300000
 isdn incoming-voice voice
 isdn map address .* plan isdn type national
```

[7] **Sip-Porofile 1** used to manipulate Invite and Cancel message coming from Telnet network. The Telnet network always send the pilot number registration on the request URI header and destination number in the TO header . CUCM use the URI header to route the call and not the TO header. These request manipulation copy the TO header user part (Called number) to the URI header user part.

[8] **Sip-Porofile 2** used to manipulate Invite coming from CUCM. The first manipulation change the PAI header server part from IP address to FQDN and second manipulation change the sendonly attribute on SDP to sendrecv during hold to hear Music On Hold.

Note: Testing was conducted at tekVizion Labs®.

```
 no cdp enable
!
ip forward-protocol nd
ip http server
no ip http secure-server
!
!
ip route 0.0.0.0 0.0.0.0 174.46.0.129
ip route 10.0.0.0 255.0.0.0 10.64.1.1!
!
!
!
!
!
control-plane
!
!
dial-peer voice 100 voip
 description Incoming dialpeer and 1+10 digits to Telnet
 destination-pattern ^1[2-9]..[2-9]......$
 session protocol sipv2
 session target sip-server
 session transport udp
 incoming called-number .T
 incoming uri to TRUNK
 voice-class codec 1
 voice-class sip early-offer forced
 voice-class sip profiles 2
 voice-class sip copy-list 1
 dtmf-relay rtp-nte
 no vad
!
dial-peer voice 101 voip
 description 10-digit local calls to Telnet
 destination-pattern ^[2-9]..[2-9]......$
 session protocol sipv2
 session target sip-server
 session transport udp
 voice-class codec 1
 voice-class sip early-offer forced
 voice-class sip profiles 2
 voice-class sip privacy id[9]
 dtmf-relay rtp-nte
 no vad
!
dial-peer voice 102 voip
 description International calls to Telnet
 destination-pattern ^011T
 session protocol sipv2
 session target sip-server
 session transport udp
 voice-class codec 1
 voice-class sip early-offer forced
 voice-class sip profiles 2
 dtmf-relay rtp-nte
 no vad
!
dial-peer voice 103 voip
 description N11 calls to Telnet
 destination-pattern ^[2-9]11$
```

[9] Enable Privacy in outgoing dial-peer using PAI header; remove this line to disable privacy.

Note: Testing was conducted at tekVizion Labs®.

```
 session protocol sipv2
 session target sip-server
 session transport udp
 voice-class codec 1
 voice-class sip early-offer forced
 voice-class sip profiles 2
 dtmf-relay rtp-nte
 no vad
!
dial-peer voice 302 voip
 description Incoming calls from primary CUCM
 huntstop
 session protocol sipv2
 session target ipv4:10.70.19.3
 incoming called-number .%
 voice-class codec 1
 voice-class sip early-offer forced
 dtmf-relay rtp-nte
 no vad
!
dial-peer voice 303 voip
 description Incoming calls from secondary CUCM
 huntstop
 session protocol sipv2
 session target ipv4:10.70.19.4
 incoming called-number .%
 voice-class codec 1
 voice-class sip early-offer forced
 dtmf-relay rtp-nte
 no vad!
!
dial-peer voice 304 voip
 description 24848519.. calls to primary CUCM
 huntstop
 preference 1
 destination-pattern ^24848519.. [10]
 session protocol sipv2
 session target ipv4:10.70.19.3[11]
 voice-class codec 1
 voice-class sip early-offer forced
 voice-class sip profiles 1
 dtmf-relay rtp-nte
 no vad
!
dial-peer voice 305 voip
 description 24848519.. calls to secondary CUCM
 huntstop
 preference 2
 destination-pattern ^24848519.. [12]
 session protocol sipv2
 session target ipv4:10.70.19.4[13]
 voice-class codec 1
```

[10] Outbound dial peer (to CUCM). The pattern here should match service provider-assigned DID numbers.

[11] Reference to CUCM primary IP address

[12] Outbound dial peer (to CUCM). The pattern here should match service provider-assigned DID numbers.

[13] Reference to CUCM secondary IP address

```
 voice-class sip early-offer forced
 voice-class sip profiles 1
 dtmf-relay rtp-nte
 no vad
!

gateway
 timer receive-rtp 1200
!
sip-ua
 credentials username 2484851990 password 7 014357530A5E51 realm BroadWorks[14]
 authentication username 2484851990 password 7 014357530A5E51 realm BroadWorks[15]
 no remote-party-id
 retry invite 2
 retry bye 2
 retry cancel 2
 retry register 10
 registrar dns:asmain.voip.telnetww.com expires 3600[16]
 sip-server dns:asmain.voip.telnetww.com[17]
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 exec-timeout 0 0
 privilege level 15
 transport input telnet
line vty 5 15
 privilege level 15
!
scheduler allocate 20000 1000
end
```

[14] Service Provider credentials for Invite challenge (User, Password and Realm)

[15] Service Provider authentication for registration challenge (User, Password and Realm)

[16] Service Provider registration signaling address and expiration timer

[17] Service Provider signaling address

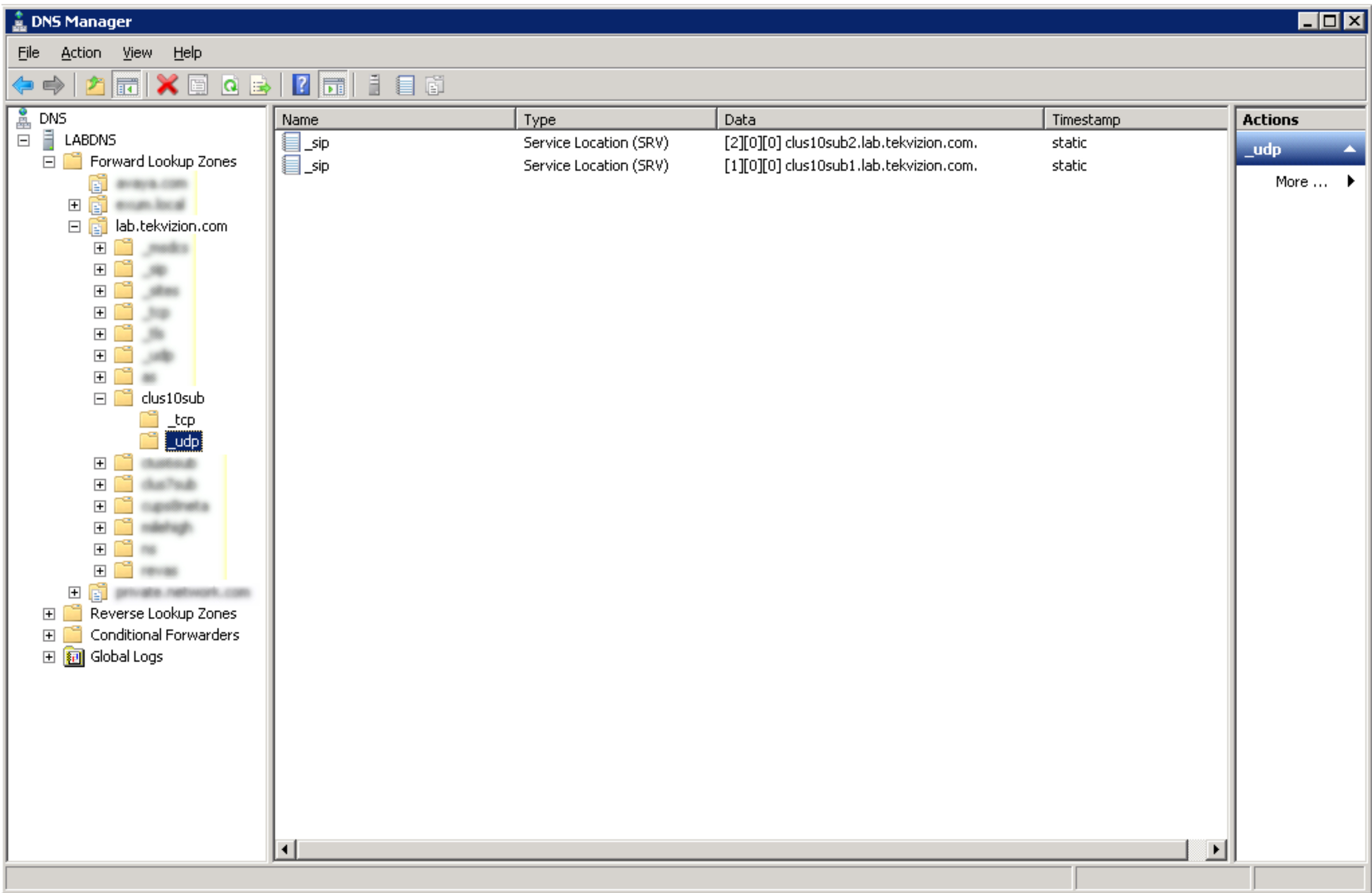
Note: Testing was conducted at tekVizion Labs®.

DNS Configuration

In a single-node cluster configuration (only one CUCM node running the CallManager service) the CUBE dial peers may simply point to the node's IP address, in which case no special DNS configuration is required. To refer to the single node by fully-qualified domain name (FQDN) a DNS A-record is required.

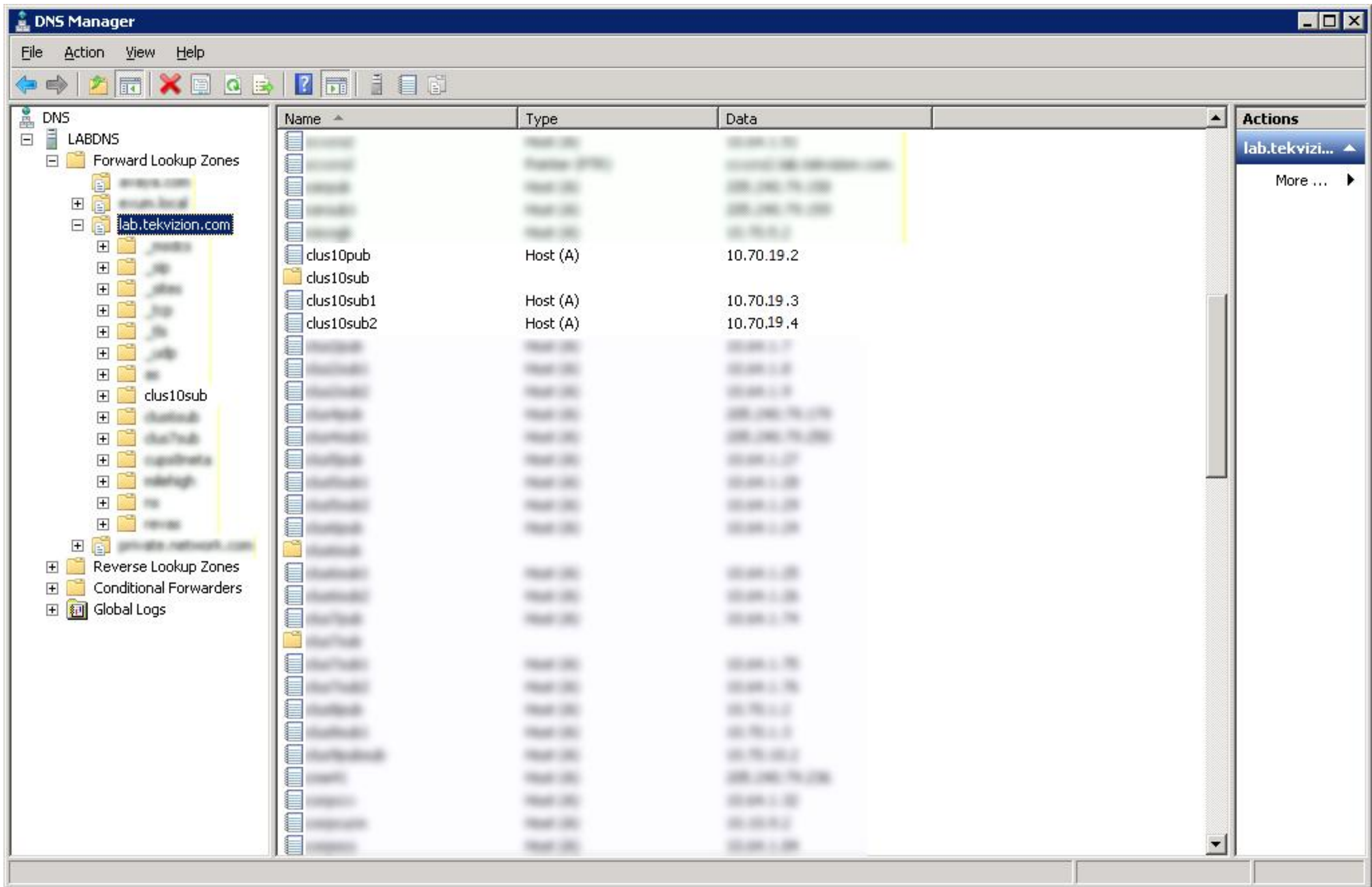
In a multi-node configuration, DNS SRV records are needed. The DNS configuration illustrated below is from a Microsoft® DNS server, although any similarly-configured, SRV-capable DNS server will work just as well.

Figure 4. DNS SRV Records



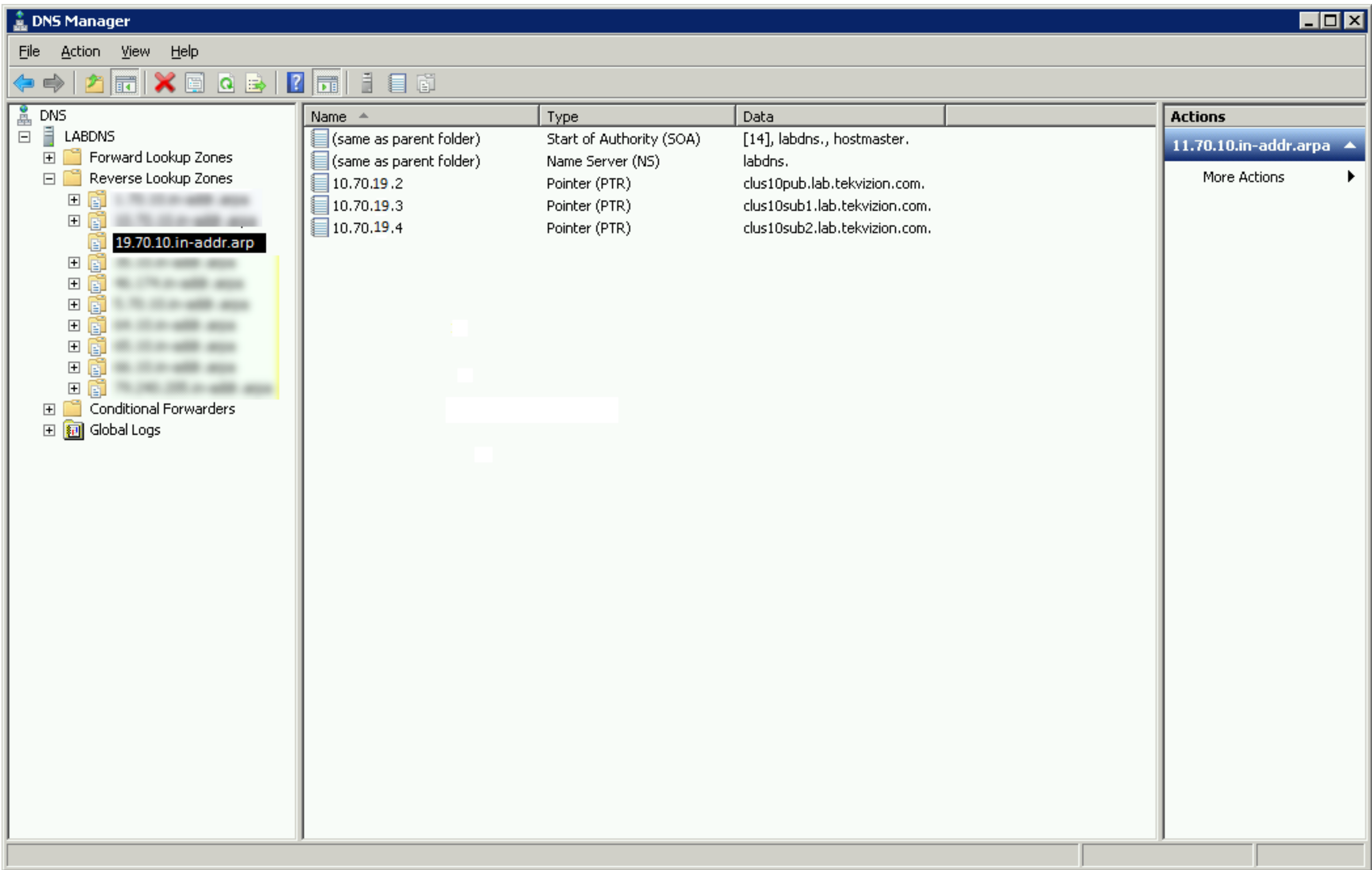
Note: Testing was conducted at tekVizion Labs®.

Figure 5. DNS A Records



Note: Testing was conducted at tekVizion Labs®.

Figure 6. DNS PTR Records



Note: Testing was conducted at tekVizion Labs®.

Configuring the Cisco Unified Communications Manager

Figure 7. Enterprise Parameters

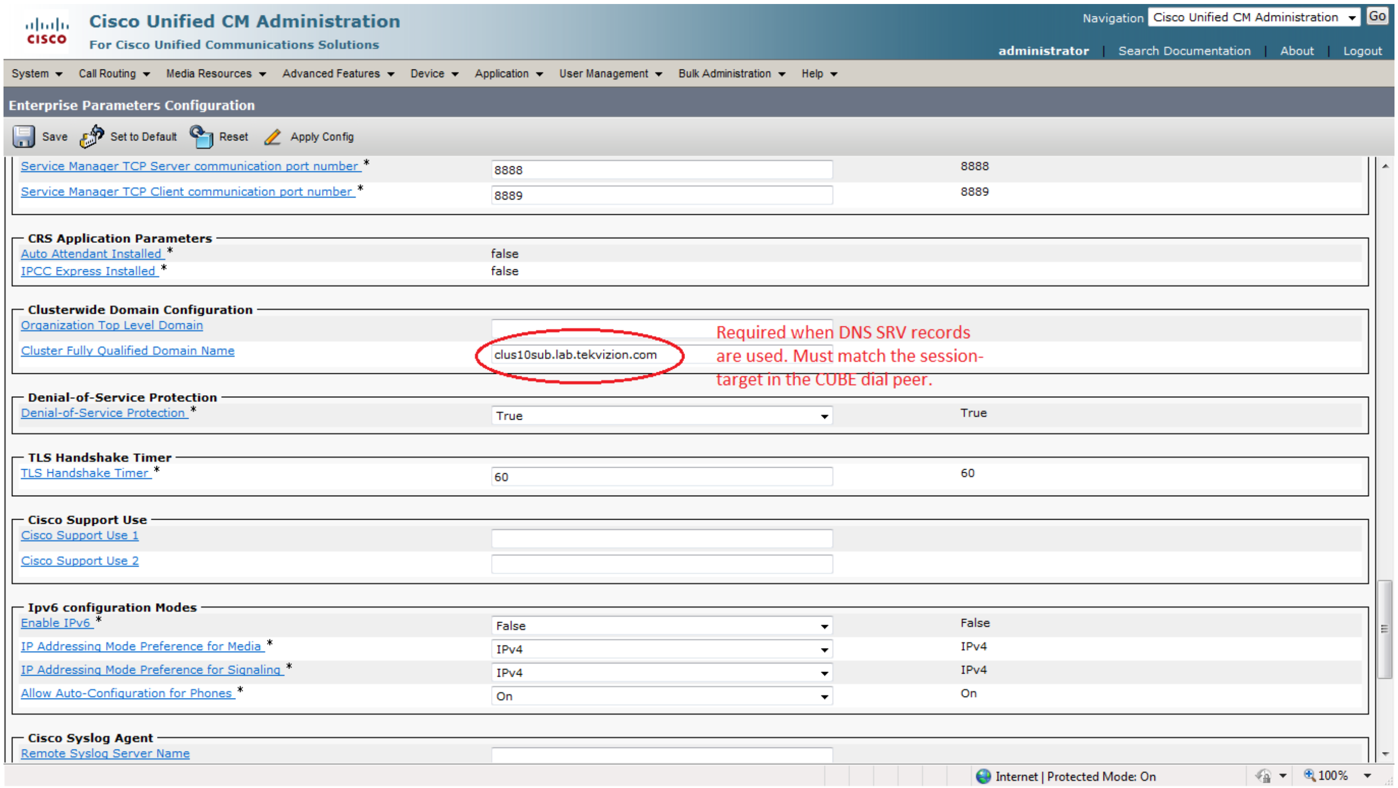
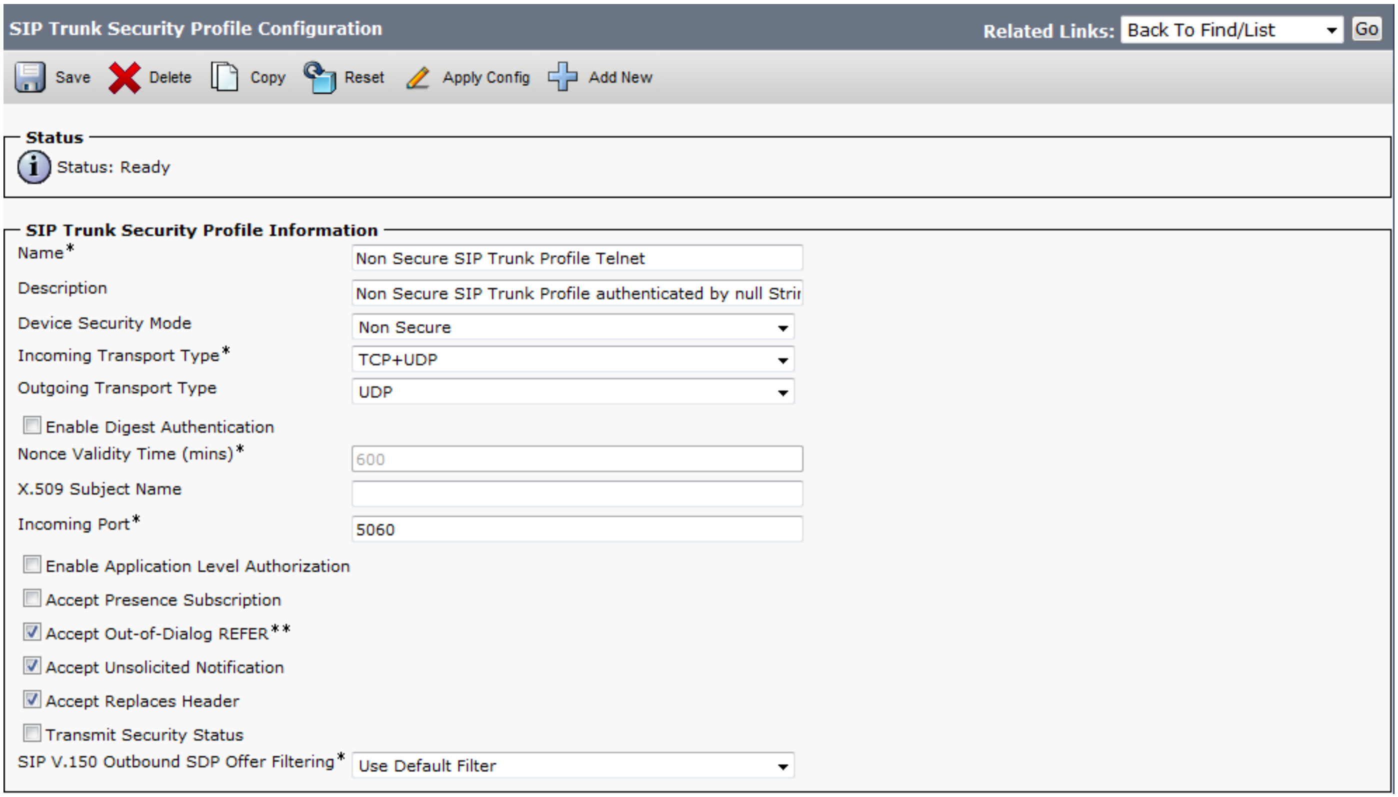
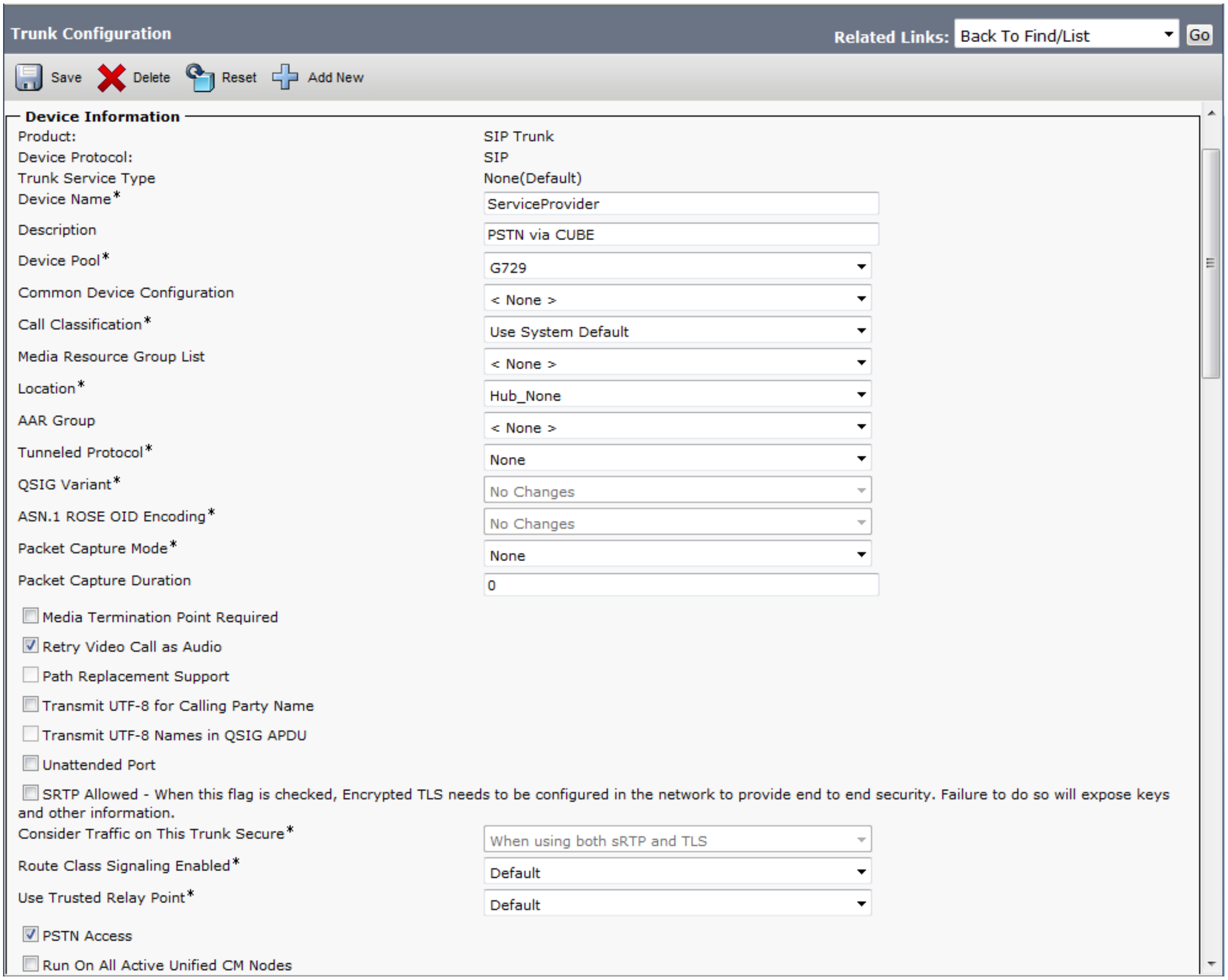


Figure 8. SIP Trunk Security Profile



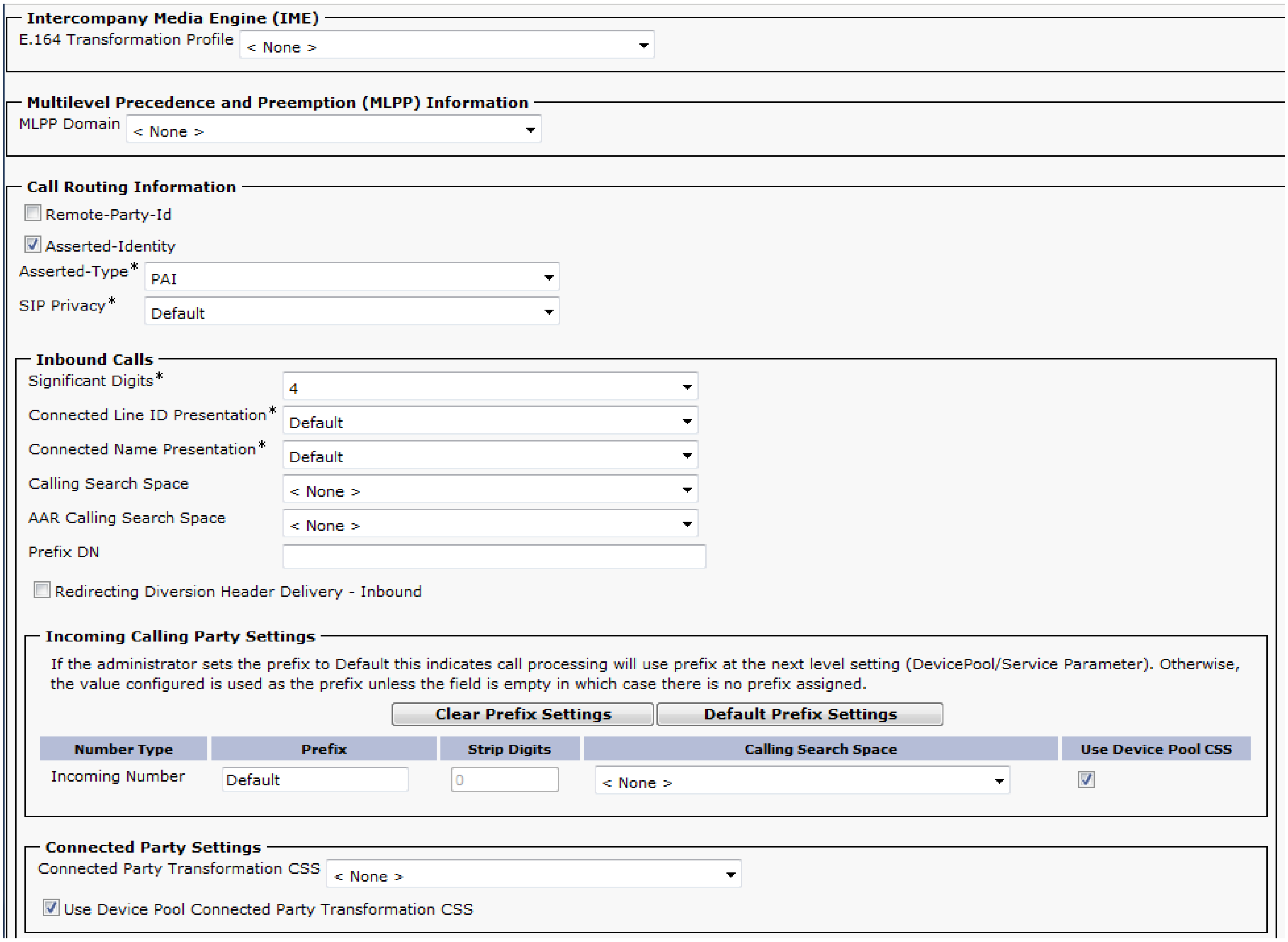
Note: Testing was conducted at tekVizion Labs®.

Figure 9. SIP Trunk to Telnet via CUBE



Note: Testing was conducted at tekVizion Labs®.

Figure 10. SIP Trunk to Telnet via CUBE (cont.)


Intercompany Media Engine (IME)

E.164 Transformation Profile < None >

Multilevel Precedence and Preemption (MLPP) Information

MLPP Domain < None >

Call Routing Information

- [ ] Remote-Party-Id
- [x] Asserted-Identity

Asserted-Type* PAI

SIP Privacy* Default

Inbound Calls

Significant Digits* 4

Connected Line ID Presentation* Default

Connected Name Presentation* Default

Calling Search Space < None >

AAR Calling Search Space < None >

Prefix DN

- [ ] Redirecting Diversion Header Delivery - Inbound

Incoming Calling Party Settings

If the administrator sets the prefix to Default this indicates call processing will use prefix at the next level setting (DevicePool/Service Parameter). Otherwise, the value configured is used as the prefix unless the field is empty in which case there is no prefix assigned.

Clear Prefix Settings | Default Prefix Settings

Number Type	Prefix	Strip Digits	Calling Search Space	Use Device Pool CSS
Incoming Number	Default	0	< None >	[x]

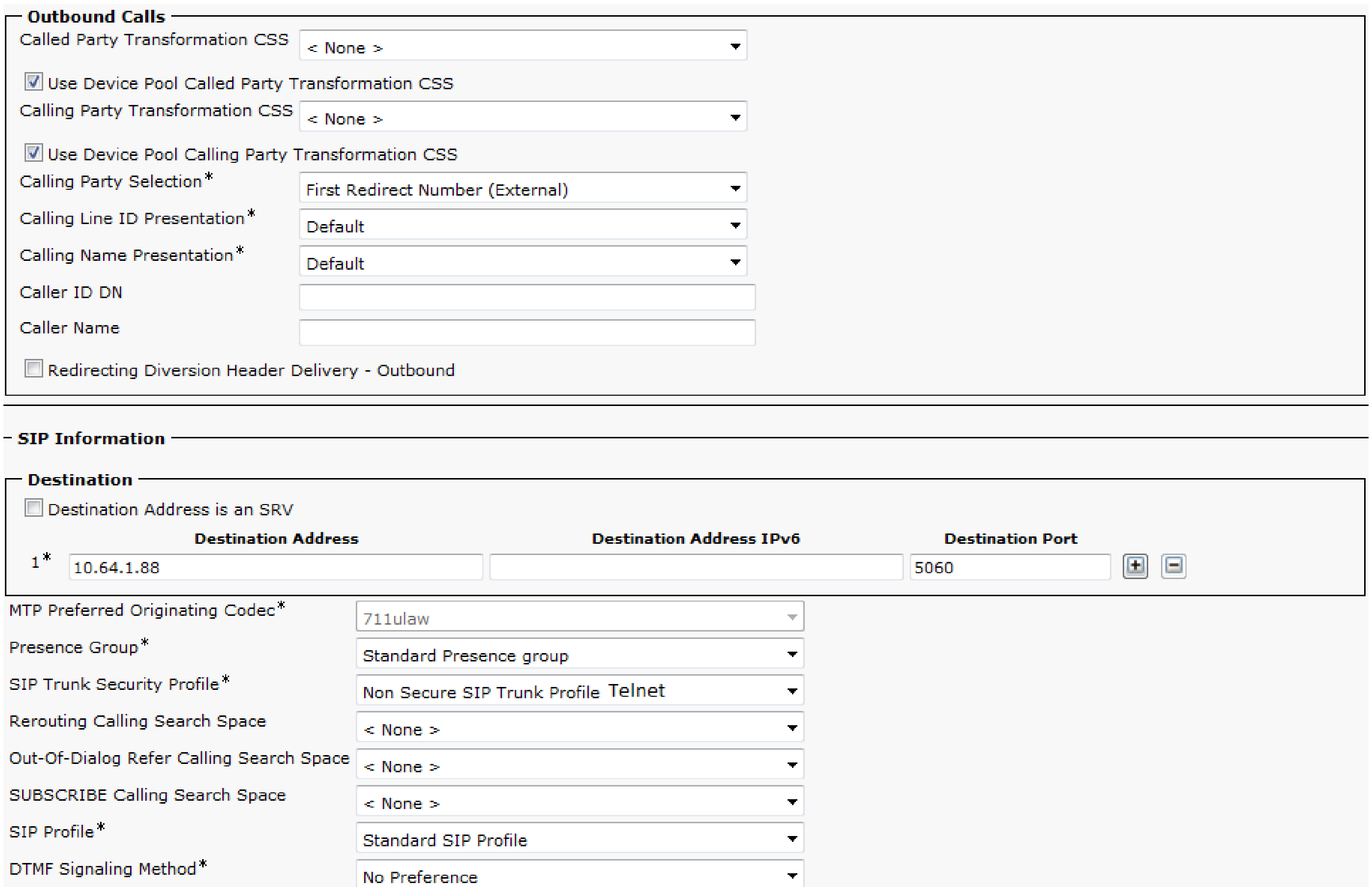
Connected Party Settings

Connected Party Transformation CSS < None >

- [x] Use Device Pool Connected Party Transformation CSS

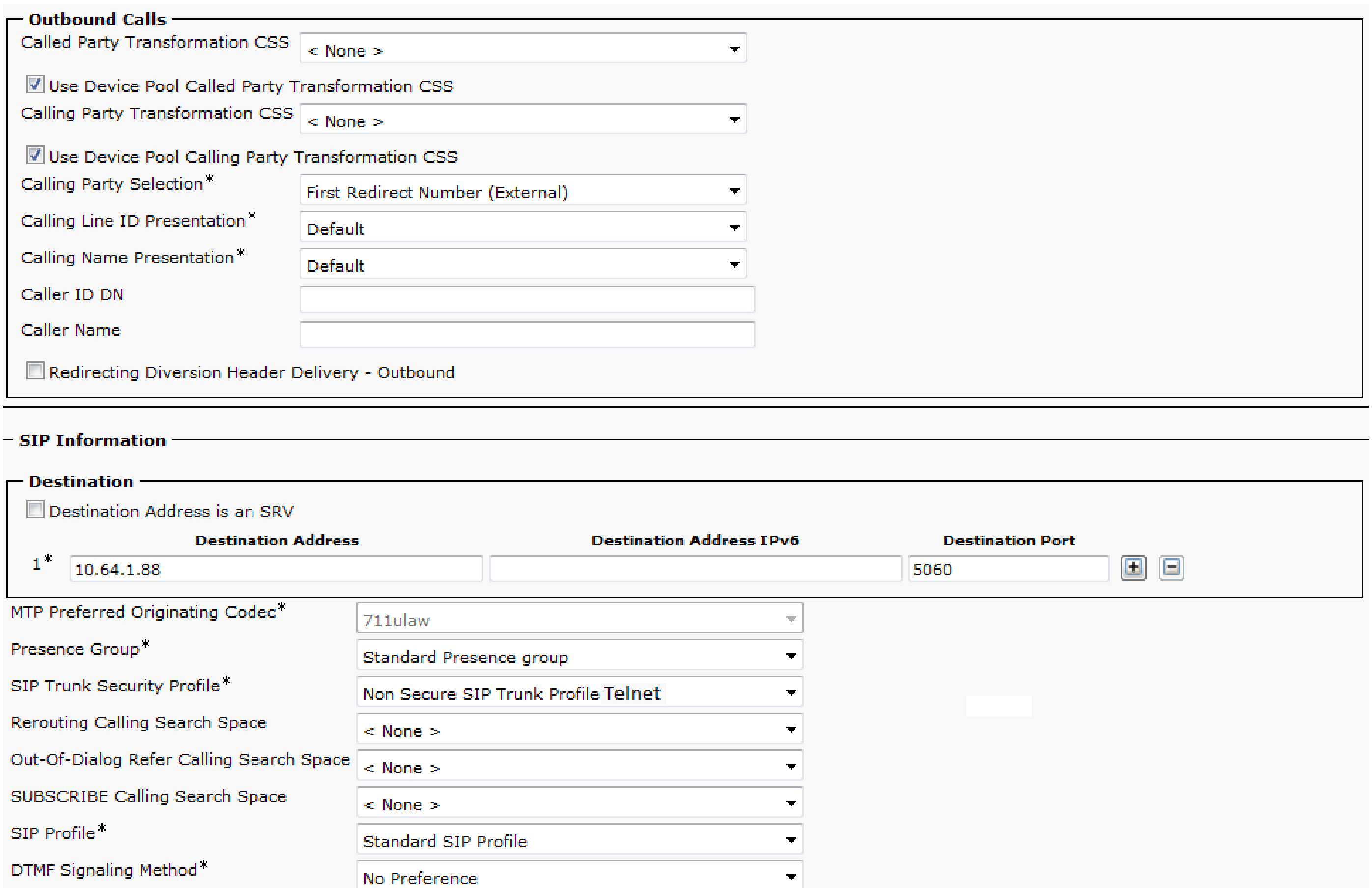
Note: Testing was conducted at tekVizion Labs®.

Figure 11. SIP Trunk to Telnet via CUBE (cont.)



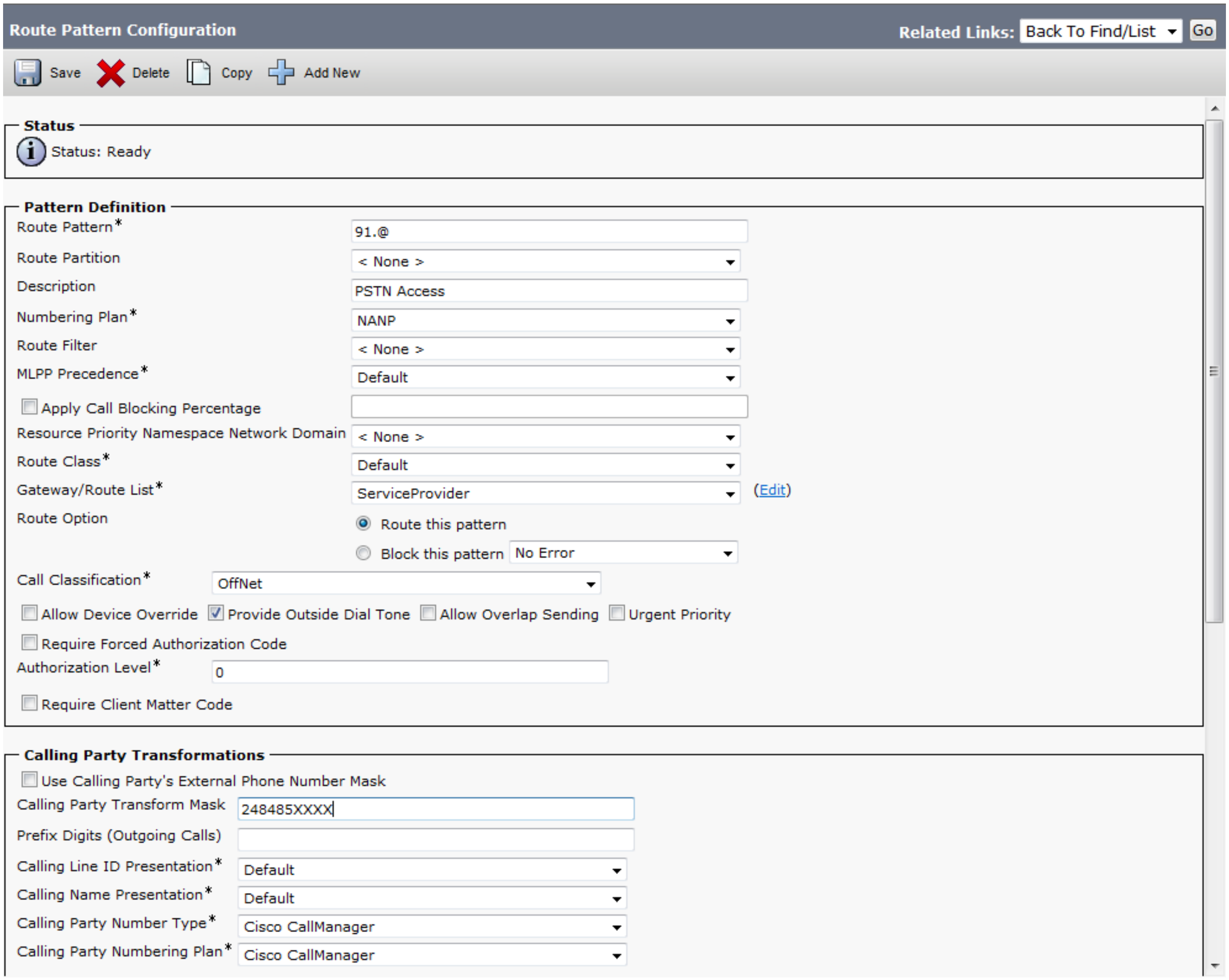
Note: Testing was conducted at tekVizion Labs®.

Figure 12. SIP Trunk to Telnet via CUBE (cont.)



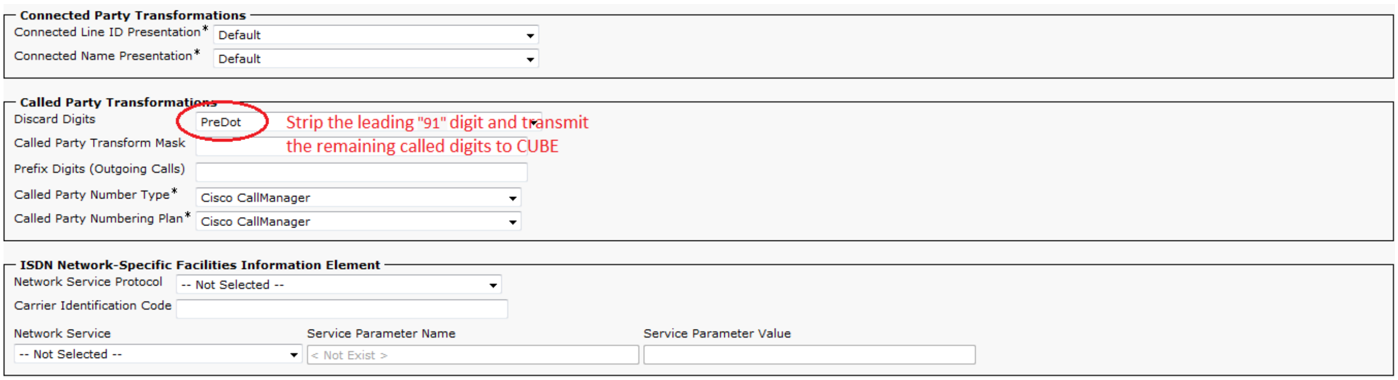
Note: Testing was conducted at tekVizion Labs®.

Figure 13. Route Pattern Configuration for SIP trunk to Telnet via CUBE



Note: Testing was conducted at tekVizion Labs®.

Figure 14. Route Pattern Configuration for SIP trunk to Telnet via CUBE (cont)



Note: Testing was conducted at tekVizion Labs®.

Acronyms

Acronym	Definitions
SIP	Session Initiation Protocol
MGCP	Media Gatew ay Control Protocol
SCCP	Skinny Client Control Protocol
Cisco UCM	Cisco Unified Communications Manager
Cisco UBE	Cisco Unified Border Element

Note: Testing was conducted at tekVizion Labs®.

Important Information

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Note: Testing was conducted at tekVizion Labs®.

Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in the USA

Note: Testing was conducted at tekVizion Labs®.