

配置与多维数据集和CUCM的语音安全功能

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[相关信息](#)

简介

本文描述如何配置在Cisco Unified Border Element (多维数据集)和Cisco Unified Communications Manager (CUCM)之间的安全。

[先决条件](#)

[要求](#)

Cisco 建议您了解以下主题：

- Cisco Unified Communications Manager (CUCM)
- Cisco Unified Border Element (多维数据集)
- 传输层安全(TLS)
- 安全实时传输协议(SRTP)
- 实时传输协议 (RTP)
- 会话初始化协议(SIP)
- 用户数据报协议 (UDP)
- 互联网电话服务提供商(ITSP)

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络实际，请保证您了解所有命令潜在影响。

背景信息

如何配置TLS和SRTP到多维数据集的RTP与CUCM

在此配置前，必须调整CUCM到与安全enable (event)的混合模式。

多维数据集作为互联网网络操作系统(IOS) Certificate Authority (CA) , CUCM证书是签字的自己。
实验室呼叫流

CP-8945电话> CUCM- (SIP/TLS) -多维数据集> (SIP/UDP) -世界其他地方模拟ITSP (RTP) >电话
SRTP在CP-8945电话和多维数据集之间
CP-8945电话号码2088年 , show命令根据从ITSP的呼叫往2088年。

配置

步骤1.为了配置时钟 , 请运行clock set命令或配置ntp。

```
Set clock 8:00:00 01 JAN 2012
Or
Ntp server x.x.x.x
ntp source FastEthernet0/0
```

```
clock timezone AEST +10
```

Configure gateway to act as http server: "ip http server"

步骤2.配置IOS PKI服务器&信任点(本地路由器作为CA)

```
crypto pki server iosca
  database level complete
  database url nvram:
  grant auto
  lifetime certificate 1800

crypto pki trustpoint iosca
  enrollment url http://10.66.75.246:80 (local Giga Ethernet ip address)
  revocation-check none
  rsakeypair iosca
```

Wait 30 seconds before issuing "no shutdown" on iosca server

```
crypto pki server iosca
  no shutdown
```

```
#####
```

```
MS-3945(cs-server)#no shut
```

```
%Some server settings cannot be changed after CA certificate generation.
```

```
% Please enter a passphrase to protect the private key
```

```
% or type Return to exit
```

```
Password:Ciscotacl23
```

```
Re-enter password:Ciscotacl23
```

```
% Generating 1024 bit RSA keys, keys will be non-exportable...
```

```
[OK] (elapsed time was 3 seconds)
```

```
Jan 7 06:30:15.825: %SSH-5-ENABLED: SSH 1.99 has been enabled% Exporting Certificate Server signing certificate and keys...
```

```
% Certificate Server enabled.
```

```
Jan 7 06:30:25.384: %PKI-6-CS_ENABLED: Certificate server now enabled.
```

```
MS-3945(cs-server)#
```

```
#####
```

步骤3.配置信任点(对于SIP和请巩固代码转换器)

注意：巩固在多维数据集注册的代码转换器为互连网络SRTP和RTP要求。

注意：巩固代码转换器没有为Agregation服务路由器(ASR)仅平台要求，集成服务路由器的(ISR) G1,G2。

```
crypto pki trustpoint cube3945
  enrollment url http://10.66.75.246:80 (local Giga Ethernet 0/1)
serial-number none
fqdn none
subject-name CN=MS-3945.eim.com (needs to match the X.509 subject name in CUCM's secure SIP
trunk profile)
ip-address none
revocation-check none
```

```
crypto pki authenticate cube3945
```

```
#####
```

```
MS-3945(config)#crypto pki authenticate cube3945
```

```
Certificate has the following attributes:
```

```
  Fingerprint MD5: 2F2D61A4 EACCC730 141B2966 7370A9AA
```

```
  Fingerprint SHA1: E6B86D4F C84B5453 8F63F019 773E1E0C 0DE5B883
```

```
% Do you accept this certificate? [yes/no]: yes
```

```
Trustpoint CA certificate accepted.
```

```
MS-3945(config)#
```

```
#####
```

```
crypto pki enroll cube3945
```

```
#####
```

```
MS-3945(config)#crypto pki enr cube3945
```

```
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
  password to the CA Administrator in order to revoke your certificate.
  For security reasons your password will not be saved in the configuration.
  Please make a note of it.
```

```
Password:Ciscotac123
```

```
Jan  7 06:31:06.884: %CRYPTO-6-AUTOGEN: Generated new 512 bit key pair
```

```
Re-enter password:Ciscotac123
```

```
% The fully-qualified domain name will not be included in the certificate
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose cube3945' command will show the fingerprint.
Jan  7 06:31:24.088: CRYPTO_PKI: Certificate Request Fingerprint MD5: 9A128490 01A60E1D
9F3C3253 48706E5F
Jan  7 06:31:24.088: CRYPTO_PKI: Certificate Request Fingerprint SHA1: 733EE8B1 DBB0F25C
595D48E3 0830047C 50DEFB16
MS-3945(config)#
Jan  7 06:31:29.156: %PKI-6-CERTRET: Certificate received from Certificate Authority
#####
```

```
crypto pki trustpoint secdsp
  enrollment url http://10.66.75.246:80
  serial-number
  revocation-check none
  rsakeypair iosca
```

```
crypto pki authenticate secdsp (same procedure as other trustpoints)
crypto pki enroll secdsp (same procedure as other trustpoints)
```

```

sccp local GigabitEthernet0/1
sccp ccm 10.66.75.246 identifier 10 version 7.0
sccp
!

!
sccp ccm group 20
  associate ccm 10 priority 1
  associate profile 20 register XCODER_IOS

!
dspfarm profile 20 transcode universal security
  trustpoint secdsp
  codec g711ulaw
  codec g711alaw
  codec g729ar8
  codec g729abr8
  maximum sessions 10
  associate application SCCP
!
telephony-service
  secure-signaling trustpoint secdsp
  tftp-server-credentials trustpoint scme
  sdspfarm units 10
  sdspfarm transcode sessions 128
  sdspfarm tag 1 XCODER_IOS
  max-ephones 50
  max-dn 300
  ip source-address 10.66.75.246 port 2000

```

The Secure transcoder must be showing up and action by following command,

MS-3945#sh sccp

```

SCCP Admin State: UP
Gateway Local Interface: GigabitEthernet0/1
  IPv4 Address: 10.66.75.246
  Port Number: 2000
IP Precedence: 5
User Masked Codec list: None
Call Manager: 10.66.75.246, Port Number: 2000
  Priority: N/A, Version: 7.0, Identifier: 10
  Trustpoint: N/A

```

```

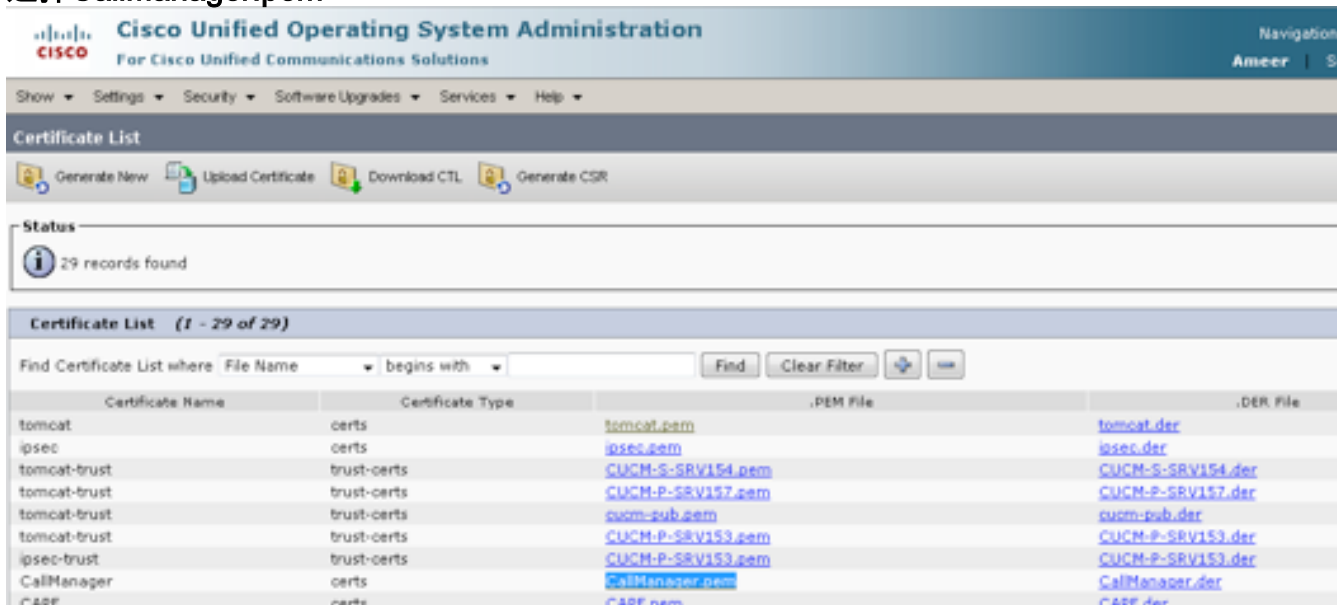
Transcoding Oper State: ACTIVE - Cause Code: NONE
Active Call Manager: 10.66.75.246, Port Number: 2443
TCP Link Status: CONNECTED, Profile Identifier: 20
Security
  Signaling Security: ENCRYPTED TLS
Media Security: SRTP
Supported crypto suites :AES_CM_128_HMAC_SHA1_32
Reported Max Streams: 20, Reported Max OOS Streams: 0
Supported Codec: g711ulaw, Maximum Packetization Period: 30
Supported Codec: g711alaw, Maximum Packetization Period: 30
Supported Codec: g729ar8, Maximum Packetization Period: 60
Supported Codec: g729abr8, Maximum Packetization Period: 60
Supported Codec: rfc2833 dtmf, Maximum Packetization Period: 30
Supported Codec: rfc2833 pass-thru, Maximum Packetization Period: 30
Supported Codec: inband-dtmf to rfc2833 conversion, Maximum Packetization Period: 30
TLS : ENABLED

```

步骤4.配置CUCM的信任点并且登记在多维数据集的CUCM证书。

```
MS-3945(config)#crypto pki trustpoint cucm50
MS-3945(ca-trustpoint)# enrollment terminal
MS-3945(ca-trustpoint)# revocation-check none
```

- 现在请登陆在CUCM (操作系统) OS管理页面：
- **安全> Certificate Management >查找**
- **选择CallManager.pem**



- 选择**下载证书**并且保存作为**.pem**文件
- 打开在记事本的**.pem**文件
- 复制从“**-----开始证书-----**”直到“**-----END证书-----**”
- 复制证书到cube3945作为示例

```
crypto pki authenticate cucm50
```

After entering the command paste the certificate and press two times enter after END CERTIFICATE.

```
#####
```

```
MS-3945(config)#crypto pki authenticate cucm-pub
```

Enter the base 64 encoded CA certificate.

End with a blank line or the word "quit" on a line by itself

```
-----BEGIN CERTIFICATE-----
```

```
MIICszCCAhygAwIBAgIIFOPHF1cCUbcwDQYJKoZIhvcNAQEFBQAwXzEWMBQGA1UE
AwwNQ1VDTS1QLVNSVjE1MzEMMAoGA1UECwwDVEFDMQ4wDAYDVQQKDAVDSVNDTzEM
MAoGA1UEBwwDQkFOMQwwCgYDVQQIDANLQVIXCzAJBgNVBAYTAK1OMB4XDTEyMTE5
NjE1MDUwM1oXDTEyMTE5NjE1MDUwM1owXzEWMBQGA1UEAwwNQ1VDTS1QLVNSVjE1
MzEMMAoGA1UECwwDVEFDMQ4wDAYDVQQKDAVDSVNDTzEMMAoGA1UEBwwDQkFOMQww
CgYDVQQIDANLQVIXCzAJBgNVBAYTAK1OMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCB
iQKBgQCRT2YXfOMgQueval6tyMCwQw0fKCDw3bqq/63atNUhSqFpswk+04GhPqxh
Pesx6bMW3E22AGWoTjrsqYTRY7TA/p2u03yPcg00PMoxNk6VN88/FLW6Ynd3rOK
TmABim1UEMVMYDFQoGhtzUxya7ZFe3vppqBnd1Urgy0q01zQzJwIDAQABo3gwdjAL
BgNVHQ8EBAMCARwwJwYDVR01BCAwHgYIKwYBBQUHAWEGCCsGAQUFBwMCBggrBgEF
BQcDBTAFBgNVHREEGDAWhhRodHRwOi8vQ1VDTS1QLVNSVjE1MzAdBgNVHQ4EFgQU
ZIIiGxzZQV0phnLrsY8Bby3jm9S0wDQYJKoZIhvcNAQEFBQADgYEAQzIvbQm8EOSU
v+bm9oykvHLmrQXjvSgSy108mC5koUurYa/a0yf0AjMwDMc8F/NArTktDyjdmmw
Oq0G1YMuMh1oyPeb41/bbc+AJxI/d/xpr0JSt1qwFI3CJjCvsWm3azC4wf1ItZNo
4gaCwzzY2UoedUA/rHrWcYod6Vl6Adw=
```

```
-----END CERTIFICATE-----
```

Certificate has the following attributes:

Fingerprint MD5: 05813269 C50FD13F 20D65A7C 0C4CD73E
Fingerprint SHA1: 8BE549A5 FB3A856F A6B3CC8B 7C30F0DF C9280288

% Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.

% Certificate successfully imported

MS-3945(config)#

#####

- 如果有超过一CallManager在CCM组中，请配置所有节点的信任点并且导入从CallManager的证书，因为上一个步骤，否则，故障切换不发生。

步骤5.导出IOS证书为了安装在CallManager CallManager

#####

MS-3945(config)#crypto pki export cube3945 pem terminal

% CA certificate:

-----BEGIN CERTIFICATE-----

```

MIIB+TCCAkwAwIBAgIBATANBgkqhkiG9w0BAQQFADAQMq4wDAYDVQQDEwVpb3Ny
YTAeFw0xMjAxMDcwNjMwMTVaFw0xNTAxMDYwNjMwMTVaMBAxDjAMBGNVBAMTBWlV
c3JhMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDDrZwLgX7LSPwS0iAgv6Zq
1AMzikR36zGH7Cai0/Mf0nZ9nmNRVskpSBhdGbjvj43/TzqcJLSricIkBnSHSVme
SXxo+gz2sGhgZBABBvjTJ86/kaVOSD9/rFJjPNdrxgA5Jdc64qUC2SKUHYGTs0Xx
alTQid2y1UOnAwpJKx8LTQIDAQABo2MwYTAPBgNVHRMBAf8EBTADAQH/MA4GA1Ud
DwEB/wQEAwIBhjAfBgNVHSMEGDAWgBQf+4wpeDVM3rkjL5LoZkjr4n4j+DAdBgNV
HQ4EFgQUH/uMKXglTN65Iy+S6GZI6+J+I/gwDQYJKoZIhvcNAQEEBQADgYEAcHvx
2hhf/eD2/mCgmcDWrh86OU5VV+0I3Eiphto6I8s+y2UhPMshF3sJ+OhDsT6T+C7U
xi0g961TxvdJDBsu7gDERioW3LuJuOKj7MNYDIbCmaoBlxCLtHsZvcnsVGrar3Jt
dVh2dnKi/O6VEzCGrjBkn6RPPXXOB9aEeQ6ts2M=
-----END CERTIFICATE-----

```

% General Purpose Certificate:

-----BEGIN CERTIFICATE-----

```

MIIBrTCCARagAwIBAgIBAJANBgkqhkiG9w0BAQQFADAQMq4wDAYDVQQDEwVpb3Ny
YTAeFw0xMjAxMDcwNjMwMTVaFw0xNTAxMDYwNjMwMTVaMBwxGjAYBgNVBAMTETAw
OjI0OjE0OkJCOjVCOkRGMFwwDQYJKoZIhvcNAQEEBQADSwAwSAJBALIXjJSbcgK3
6c4EnOs/FDrqktwHXQhwncAh2N3k4LghdwAdsQFXGtHjeFJWA6TBm/fLibLD4fW8
eoacG7fpJJKCAwEAANPME0wCwYDVR0PBAQDAgWgMB8GA1UdIwQYMBaAFB/7jC14
NUzeuSMvkuhMSovifiP4MB0GA1UdDgQWBBSW11Md2rFbqzF0IuicijOJ15PnPDAN
BgkqhkiG9w0BAQQFAA0BgQCZeTK4TeNrtoQ3/3eaCD7sL/RNica8ArbNOn2KcCxyO
WmtH8xRs4Hm9lw4K4o93D3mgAP6JLAB6RN4LdzFm5S800YXTDYoeQ/kO9i9RrTFq
ARbdZRuULb02tgRbJyHngQ5dV7C7hqwR4CfjJeQI1UQWSibiyKT0mN8o5n/1B37G
GQ==
-----END CERTIFICATE-----

```

MS-3945(config)#

#####

- 复制证书并且保存在记事本， cube3945g.pem文件。

注意：需要的仅通用证书

- 上传IOS CA证书作为CallManager托拉斯。
- 导航对CUCM OS管理页面
- 安全> Certificate Management >加载证书

步骤6.配置Cube3945和CUCM Secure电话的CP-8945

在多维数据集

#####

MS-3945(config)#crypto pki export cube3945 pem terminal

% CA certificate:

-----BEGIN CERTIFICATE-----

MIIB+TCCAkwAgIBAgIBATANBgkqhkiG9w0BAQQFADAQMq4wDAYDVQDEwVpb3NyYTAeFw0xMjAxMDcwNjMwMTVaFw0xNTAxMDYwNjMwMTVaMBAxDjAMBgNVBAMTBWlv c3JhMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDDrZwLgX7LSPwS0iAgv6Zq 1AMzikR36zGH7Cai0/Mf0nZ9nmNRVskpSBhDgbjvj43/TzqcJLSricIkBnSHSVme SXxo+gz2sGhgZBABBvjTJ86/kaVOSD9/rFJjPNdrxgA5Jdc64qUC2SKUHYGTs0Xx a1TQiD2ylUOnAwpJKx8LTQIDAQABo2MwYTAPBgNVHRMBAf8EBTADAQH/MA4GA1Ud DwEB/wQEAWIBhjAfBgNVHSMGDAWgBQf+4wpeDVM3rkjL5LoZkjr4n4j+DAdBgNV HQ4EFgQUH/uMKXglTN65Iy+S6GZI6+J+I/gwDQYJKoZIhvcNAQEEBQADgYEAcHvx 2hhF/eD2/mCgmcDWrh86OU5VV+0I3Eiphto6I8s+y2UhPMshF3sJ+OhDsT6T+C7U xi0g961TxvdJDBsu7gDERioW3LuJuOKj7MNYDIbCmaoBlxCLtHsZvcnsVGrar3Jt dVh2dnKi/O6VEzCGrjBkn6RPPXXOB9aEeQ6ts2M=

-----END CERTIFICATE-----

% General Purpose Certificate:

-----BEGIN CERTIFICATE-----

MIIBrTCCARagAwIBAgIBAJANBgkqhkiG9w0BAQQFADAQMq4wDAYDVQDEwVpb3NyYTAeFw0xMjAxMDcwNjMwMTVaFw0xNTAxMDYwNjMwMTVaMBAwGjAYBgNVBAMTETAw OjI0OjE0OkJCOjVCOkRGMFwwDQYJKoZIhvcNAQEEBQADSwAwSAJBALixjJSbcgK3 6c4EnOs/FDrqKtwhXQhwncah2N3k4LghdwAdsQFXGtHjeFJWA6TBm/fLibLD4fW8 eoacG7fpJJKCAwEAAANPME0wCwYDVR0PBAQDAGWgMB8GA1UdIwQYMBaAFB/7jCl4 NUzeuSMvkuhMSovifiP4MB0GA1UdDgQWBBSW11Md2rFbqZf0IuicijOJ15PnPDAN BgkqhkiG9w0BAQQFAA0BgQCZetK4TeNrtoQ3/3eaCD7sL/RNic8aRbNOn2KcCxyO WmtH8xRs4Hm9lw4K4o93D3mgAP6JLAB6RN4LdzFm5S800YXTDY0eQ/k09i9RrTFq ARbdZRULb02tgRbJyHngQ5dV7C7hqwr4CfjJeQI1UQWSibiyKT0mN8o5n/1B37G GQ==

-----END CERTIFICATE-----

MS-3945(config)#

#####


在CUCM

- 在CUCM的寄存器CP-8945在安全模式。
- 创建CP-8945的一安全SCCP配置文件
- 选择安全配置文件在CP-8945的配置下。

Phone Security Profile Configuration

 Save  Delete  Copy  Reset  Apply Config  Add New

- Status

 Status: Ready

- Phone Security Profile Information

Product Type: Cisco 8945

Device Protocol: SCCP

Name*

Description

Device Security Mode

TFTP Encrypted Config

- Phone Security Profile CAPF Information

Authentication Mode*

Key Size (Bits)*

Note: These fields are related to the CAPF Information settings on the Phone Configuration page.

Protocol Specific Information

Packet Capture Mode*

Packet Capture Duration

Presence Group*

Device Security Profile*

SUBSCRIBE Calling Search Space

Unattended Port

Require DTMF Reception

RFC2833 Disabled

- 保存并且重置CP-8945配置，保证它注册好
- 应用在SIP中继的安全SIP配置文件往多维数据集

SIP Trunk Security Profile Configuration

Save
 Delete
 Copy
 Reset
 Apply Config
 Add New

Status

Status: Ready

SIP Trunk Security Profile Information

Name*

Description

Device Security Mode

Incoming Transport Type*

Outgoing Transport Type

Enable Digest Authentication

Nonce Validity Time (mins)*

X.509 Subject Name

Incoming Port*

Enable Application level authorization

Accept presence subscription

Accept out-of-dialog refer**

Accept unsolicited notification

Accept replaces header

Transmit security status

Allow charging header

SIP V.150 Outbound SDP Offer Filtering*

• SIP中继配置

Media Termination Point Required
 Retry Video Call as Audio
 Path Replacement Support
 Transmit UTF-8 for Calling Party Name
 Transmit UTF-8 Names in QSIG APDU
 Unattended Port
 SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information.
 Consider Traffic on This Trunk Secure*
 Route Class Signaling Enabled*
 Use Trusted Relay Point*
 PSTN Access
 Run On All Active Unified CM Nodes

-SIP Information-

Destination

Destination Address is an SRV

Destination Address	Destination Address IPv6	Destination Port
1* 10.66.75.246		5061

MTP Preferred Originating Codec* G729/G729a

Presence Group* Standard Presence group

SIP Trunk Security Profile* Secure SIP Trunk Profile

Rerouting Calling Search Space <None >

Out-Of-Dialog Refer Calling Search Space <None >

SUBSCRIBE Calling Search Space <None >

SIP Profile* TEST_SIP_Profile

DTMF Signaling Method* No Preference

- 使用测试呼叫，您能使用show命令为了验证呼叫在SRTP对多维数据集的RTP，并且在CP-8945屏幕的衣物柜镜像确认，有在电话和多维数据集之间的SRTP

MS-3945#sh sccp conn

sess_id	conn_id	stype	mode	codec	sport	rport	ripaddr	conn_id_tx
458757	20	s-xcode	sendrecv	g711u	16770	2000	10.66.75.246	
458757	24	xcode	sendrecv	g711u	16768	2000	10.66.75.246	

Total number of active session(s) 1, and connection(s) 2

MS-3945#sh call active voice brief

```
<ID>: <CallID> <start>ms.<index> (<start>) +<connect> pid:<peer_id> <dir> <addr> <state>
dur hh:mm:ss tx:<packets>/<bytes> rx:<packets>/<bytes> dscp:<packets violation> media:<packets
violation> audio tos:<audio tos value> video tos:<video tos value>
IP <ip>:<udp> rtt:<time>ms pl:<play>/<gap>ms lost:<lost>/<early>/<late>
delay:<last>/<min>/<max>ms <codec> <textrelay> <transcoded>

media inactive detected:<y/n> media cntrl rcvd:<y/n> timestamp:<time>

long duration call detected:<y/n> long duration call duration :<sec> timestamp:<time>
MODEMPASS <method> buf:<fills>/<drains> loss <overall%> <multipkt>/<corrected>
last <buf event time>s dur:<Min>/<Max>s
FR <protocol> [int dlci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
<codec> (payload size)
ATM <protocol> [int vpi/vci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
<codec> (payload size)
Tele <int> (callID) [channel_id] tx:<tot>/<v>/<fax>ms <codec> noise:<l> acom:<l> i/o:<l>/<l>
dBm
MODEMRELAY info:<rcvd>/<sent>/<resent> xid:<rcvd>/<sent> total:<rcvd>/<sent>/<drops>
speeds(bps): local <rx>/<tx> remote <rx>/<tx>
Proxy <ip>:<audio udp>,<video udp>,<tcp0>,<tcp1>,<tcp2>,<tcp3> endpt: <type>/<manf>
bw: <req>/<act> codec: <audio>/<video>
tx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>
rx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>

Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 2
Multicast call-legs: 0
Total call-legs: 4
0 : 32138 423566780ms.1 (02:08:15.881 UTC Tue Feb 5 2013) +2270 pid:2088 Answer 1005 active
dur 00:00:35 tx:1761/281760 rx:1753/280480 dscp:0 media:0 audio tos:0xB8 video tos:0x0
```

IP 10.66.75.178:24714 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off Transcoded: Yes
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a

0 : 32139 423566790ms.1 (02:08:15.891 UTC Tue Feb 5 2013) +2250 pid:1006 Originate 2088 active
dur 00:00:35 tx:1753/287492 rx:1761/288804 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 10.66.75.76:22512 SRTP: on rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off Transcoded: Yes
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a

0 : 32142 423569050ms.1 (02:08:18.151 UTC Tue Feb 5 2013) +0 pid:0 Originate connecting
dur 00:00:35 tx:1761/281760 rx:1753/280480 dscp:0 media:0 audio tos:0x0 video tos:0x0
IP 10.66.75.246:2000 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off Transcoded: No
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a

0 : 32144 423569050ms.2 (02:08:18.151 UTC Tue Feb 5 2013) +0 pid:0 Originate connecting
dur 00:00:35 tx:1753/287492 rx:1761/288804 dscp:0 media:0 audio tos:0x0 video tos:0x0
IP 10.66.75.246:2000 SRTP: on rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off Transcoded: No
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a

Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 2
Multicast call-legs: 0
Total call-legs: 4

相关信息

- [CUCM安全指南](#)
- [多维数据集配置指南](#)