

Unified Border Element (CUBE)与统一视频会议(CUVC) IVR的配置示例

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置](#)

[网络图](#)

[图表呼叫流](#)

[配置](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

基于IP的视频通信的采用在企业内顺利进行。在今天经济环境，用户使用视频中频繁地作为一个工具的公司内部的通信与是此的采用的主要优点收益在员工生产力和工作效率上。

多数企业基于IP的视频通信通讯网络今天是类似海岛相对使用更旧的综合业务数字网络(ISDN)技术被互联的其他这样企业网络。ISDN为所有额外企业或额外校园通信是非常常用的与其它事项，并且，在某些情况下，甚而与远端分支机构在企业内。基于IP的视频通信的广远的好处可能真实现与端到端IP连通性在或组织之内实现企业对企业(B2B)通信。这要求从ISDN的一转换到横断互联网而不是PSTN，启用公司内部和B2B通信的一个较低花费的聚合的选项的基于IP的解决方案。

批发转换从ISDN电路到IP连接通过互联网不是一琐细的职业。ISDN电路和附加ISDN到基于IP的视频通信世界的视频网关，是一个广泛配置的，时间证明和委托的解决方案。尽管在适应下一代视频通信服务的限制，ISDN仍然规定新的解决方案，当考虑到安全、保密性、计费 and 分界时的标准。新的解决方案必须提供企业和服务提供商的相似的service-level保证能他们把一个可行的选择视为。企业因而需要方式维护与ISDN产生关联的所有好处，当利用扩大在企业之外时的基于IP的视频通信效率。

此配置示例突出显示Cisco Unified Border Element (多维数据集)的功能和特别地说明多维数据集如何支持在互联网驻留某处通过IP地址拨号到一个多点控制单元的终端的能力(MCU)或终端是在公司防火墙后。此功能陈列空呼叫编号覆盖功能可用在12.4(22)YB版本多维数据集1.3和IVR功能可用在Cisco Unified视频会议(CUVC) MCU的5.6版本。本文包含配置推荐和可能的出发点开始此演变的企业。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 基础知识如何配置和使用Cisco IOS语音(例如Dial Peer)
- 基础知识如何配置和使用多维数据集
- 基本的了解防火墙如何工作

使用的组件

本文的信息根据：

- 在Cisco 2800路由器运作并且使用Cisco IOS版本12.4.22(YB)或Cisco IOS版本15.0.1M的Cisco Unified Border Element和Cisco IOS网守
- Cisco IP运行软件版本5.6或以上的视频会议3545解决方案

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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

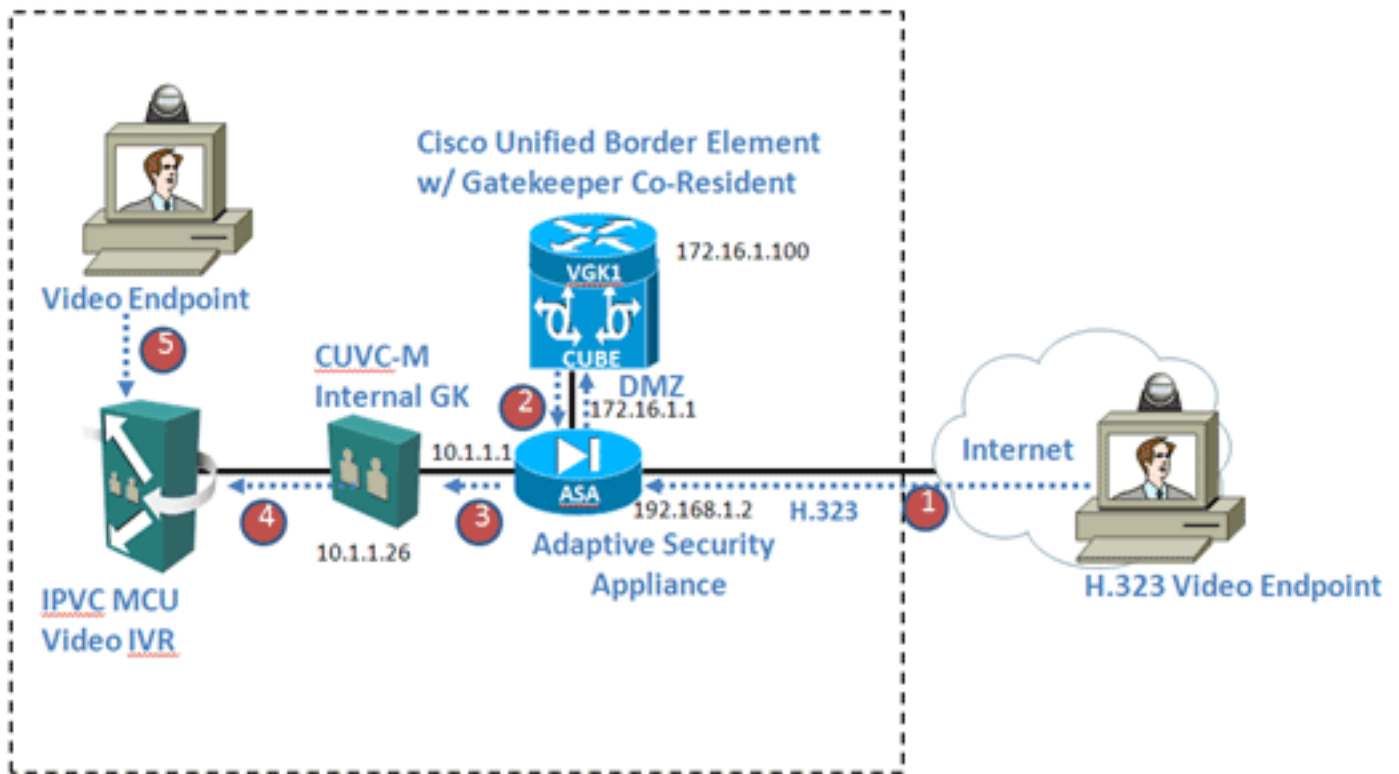
配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用[命令查找工具](#)（[仅限注册用户](#)）可获取有关本部分所使用命令的详细信息。

网络图

此图表显示多维数据集安全地拨号到用户网络的外部终端通过一个内部终端IP地址。



图表呼叫流

1. 在互联网的一个外部终端拨打多维数据集(192.168.1.2)的一个公共IP地址加入在一个内部Cisco多点控制单元的视频会议(MCU)驻留。H.323呼叫建立消息到达多维数据集由于1720一个最初的针孔被配置的TCP端口的在是防火墙为网络提供安全边界的Cisco可适应的安全工具(ASA)。在本例中，多维数据集有一个专用IP地址，因此外部终端瞄准的公开可路由地址是ASA的静态NAT(网络地址转换)进行的结果。**注意：**用于示例的目的，Cisco在文档使用仅专用IP地址空间。
2. 因为流入SETUP信息不包括多维数据集通常瞄准呼叫的下个段的通常拨号数位将，多维数据集使用空呼叫**编号覆盖**配置命令(1234567890)配置的位。使用此地址，呼叫建立消息进行往内部用户网络。
3. ASA有支持两个的针孔呼叫的此阶段：一允许多维数据集的通过CUVC-M内部关守功能查寻所需的地址和一个允许结果SETUP信息从多维数据集达到CUVC-M建立呼叫到根据E.164地址的MCU被配置在多维数据集的Dial Peer。使用在ASA的H.323检查功能，剩余的信令和媒体流TCP和UDP连接根据从呼叫建立信令搜集的信息动态地被打开。
4. CUVC-M内部网守路由呼叫对包括一个新的视频IVR功能显示一个图形选项菜单给外部用户的IPVC-MCU。此菜单通过输入DTMF音浏览通过呼叫的终端的拨号填充或遥控。若被设定终端用户选择会议ID从**加入conference**菜单选项然后输入必要的密码。
5. 内部视频端点通过拨打会议ID加入会议和外部终端一样。

配置

本文档使用以下配置：

- [多维数据集配置示例](#)
- [ASA配置示例](#)

多维数据集配置

```

!
version 12.4
service timestamps debug datetime localtime
service timestamps log datetime msec
service password-encryption
service sequence-numbers
!
hostname cube1
!
boot-start-marker
boot system flash:c2800nm-adventerprisek9_ivs-mz.124-
22.YB.bin
boot-end-marker
!
ip source-route
!
!
multilink bundle-name authenticated
!
!
!
voice service voip
    allow-connections h323 to h323
    h323
    emptycapability
    null-called-number override 1234567890
    h225 start-h245 on-connect
    call start slow
    h245 passthru all
!
!
!
voice class h323 10
!
!
voice-card 0
!
!
!
!
interface GigabitEthernet0/0
    ip address 172.16.1.100 255.255.255.0
    ip route-cache same-interface
    duplex auto
    speed auto
    h323-gateway voip interface
    h323-gateway voip id vgk1 ipaddr 172.16.1.100 1719
priority 1
!--- vgk1 defines zone the cube to register with the
local Gatekeeper service h323-gateway voip h323-id cube1
!--- Defines the ID of CUBE h323-gateway voip tech-
prefix 1# h323-gateway voip bind srcaddr 172.16.1.100 !
! ip forward-protocol nd ip route 0.0.0.0 0.0.0.0
172.16.1.1 ip http server no ip http secure-server ! ! !
! dial-peer voice 1 voip destination-pattern .T !--- To
match outbound call leg to send to GK process session
target ras incoming called-number . !--- For inbound
call leg codec transparent ! ! gateway timer receive-rtp
1200 ! ! ! gatekeeper zone local vgk1 cisco.com zone
remote CUVCM cisco.com 10.1.1.26 invia vgk1 outvia vgk1
enable-intrazone zone prefix CUVCM 1234567890 gw-type-
prefix 1#* default-technology no use-proxy GK1 default

```

```
inbound-to terminal no use-proxy GK1 default outbound-
from terminal bandwidth interzone default 1000000 no
shutdown ! end
```

ASA 配置

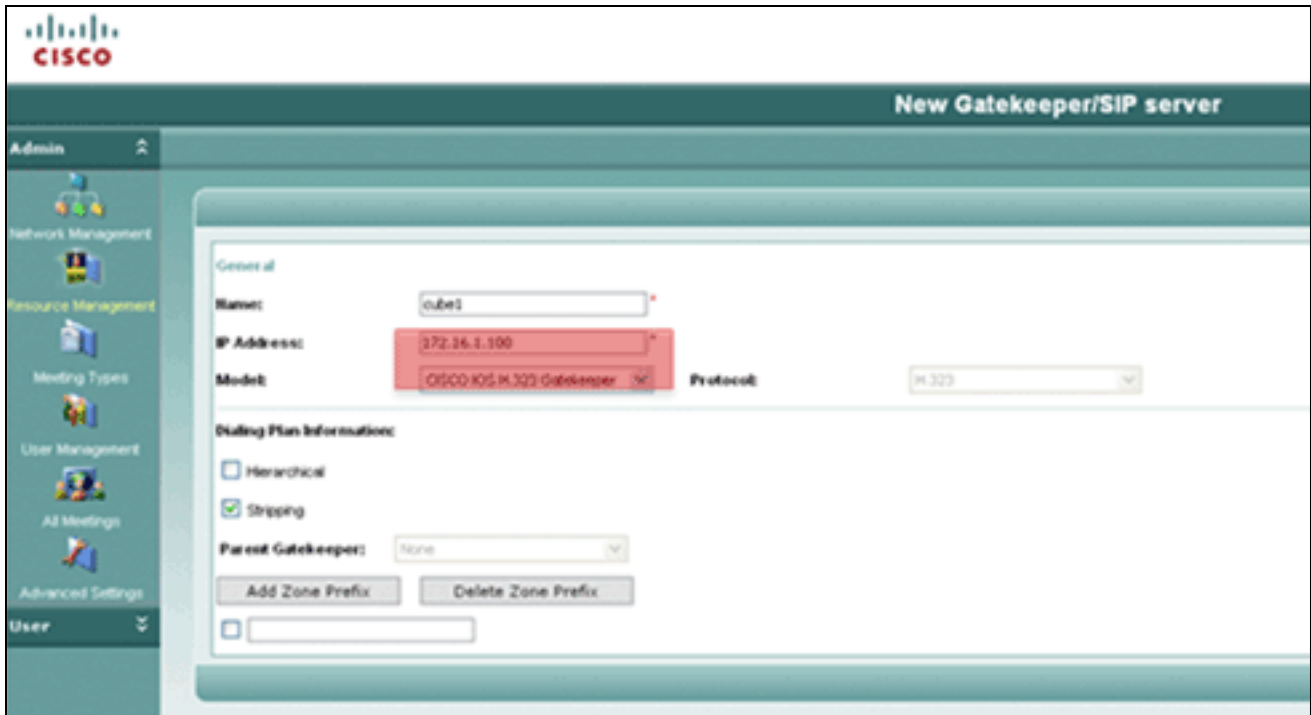
```
ASA Version 8.2(1)
!
!--- This is only a portion of the ASA config. !--- In a
typical production scenario, these commands would !---
be in addition to the current security policies
configured. ! interface Ethernet0/0 no nameif no
security-level no ip address ! interface Ethernet0/0.2
vlan 2 nameif inside security-level 100 ip address
10.1.1.1 255.255.255.0 ! interface Ethernet0/0.12 vlan
12 nameif dmz security-level 50 ip address 172.16.1.1
255.255.255.0 ! interface Ethernet0/0.500 vlan 500
nameif outside security-level 0 ip address 192.168.1.2
255.255.255.0 ! boot system disk0:/asa821-k8.bin ftp
mode passive clock timezone CDT -6 access-list dmz-in
extended permit icmp any any access-list dmz-in extended
permit udp host 172.16.1.100any eq 1719 access-list dmz-
in extended permit tcp host 172.16.1.100any eq h323 !---
The access list allows CUBE address lookups and call !--
- signaling respectively to get to the interior of the
network. ! access-list outside_access_in extended permit
icmp any any access-list outside_access_in extended
permit tcp any host 192.168.1.2 eq h323 access-list
outside_access_in extended permit udp any host
192.168.1.2 eq 1719 !--- The access list allows exterior
call setups and address !--- look ups respectively to
get to the CUBE. ! ! access-list inside-to-DMZ-exemption
extended permit ip 10.0.0.0 255.0.0.0 10.150 .150.0
255.255.255.0 !--- This access list prevents the global
NAT translation intended !--- for the outside interface
from being used on the conversations !--- between
internal endpoints and CUBE. ! mtu inside 1500 mtu dmz
1500 mtu outside 1500 nat-control global (outside) 1
192.168.1.5-192.168.1.100 netmask 255.255.255.0 !---
Note that the general NAT pool should not overlap the !-
-- ASA interface nor the static NAT used for CUBE. ! nat
(inside) 0 access-list inside-to-DMZ-exemption nat
(inside) 1 0.0.0.0 0.0.0.0 nat (dmz) 1 172.168.1.0
255.255.255.0 static (dmz,outside) 192.168.1.2
172.16.1.100 netmask 255.255.255.255 !--- The previous
statement is what establishes the publicly !--- routed
address for CUBE on the outside interface. ! access-
group dmz-in in interface dmz access-group
outside_access_in in interface outside route inside
10.0.0.0 255.255.255.0 10.1.1.2 1 route outside 0.0.0.0
0.0.0.0 192.168.1.254 1 !--- These two static route
statements assume the existence of !--- a next hop
router on both inside and outside interfaces. ! timeout
xlate 3:00:00 timeout conn 1:00:00 half-closed 0:10:00
udp 0:10:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323
0:10:00 h225 1:00:00 mgcp 0:10:00 mgcp-pat 0:10:00 !---
Note: It is a good idea to increase the H.225 timeout.
Not all endpoints !--- send enough traffic on this
connection to keep it alive. The H.225 command !---
includes the H.245 attributes.
!
policy-map global_policy
```

```
class inspection_default
  inspect h323 h225
  inspect h323 ras
```

验证

使用本部分可确认配置能否正常运行。

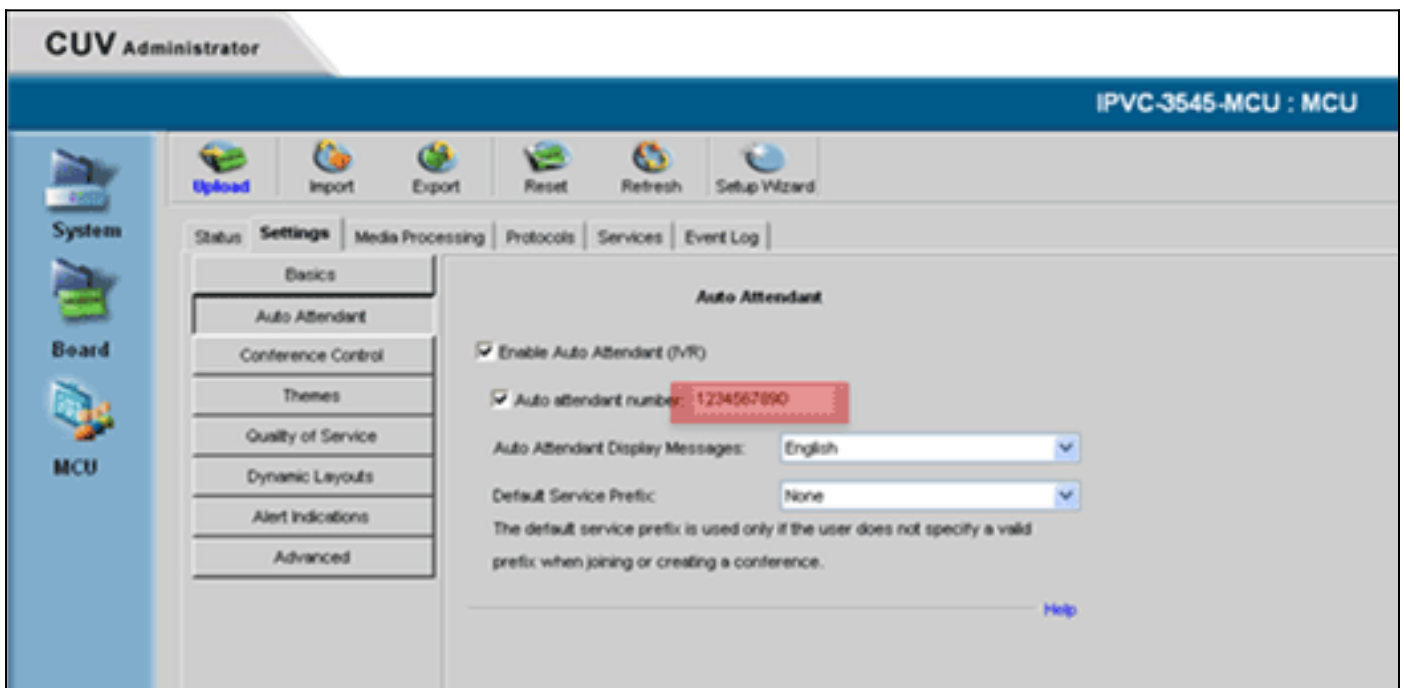
此镜像显示被添加到Cisco Unified Videoconferencing Manager的Cisco IOS网守。Cisco IOS网守型号在下拉列表选择。



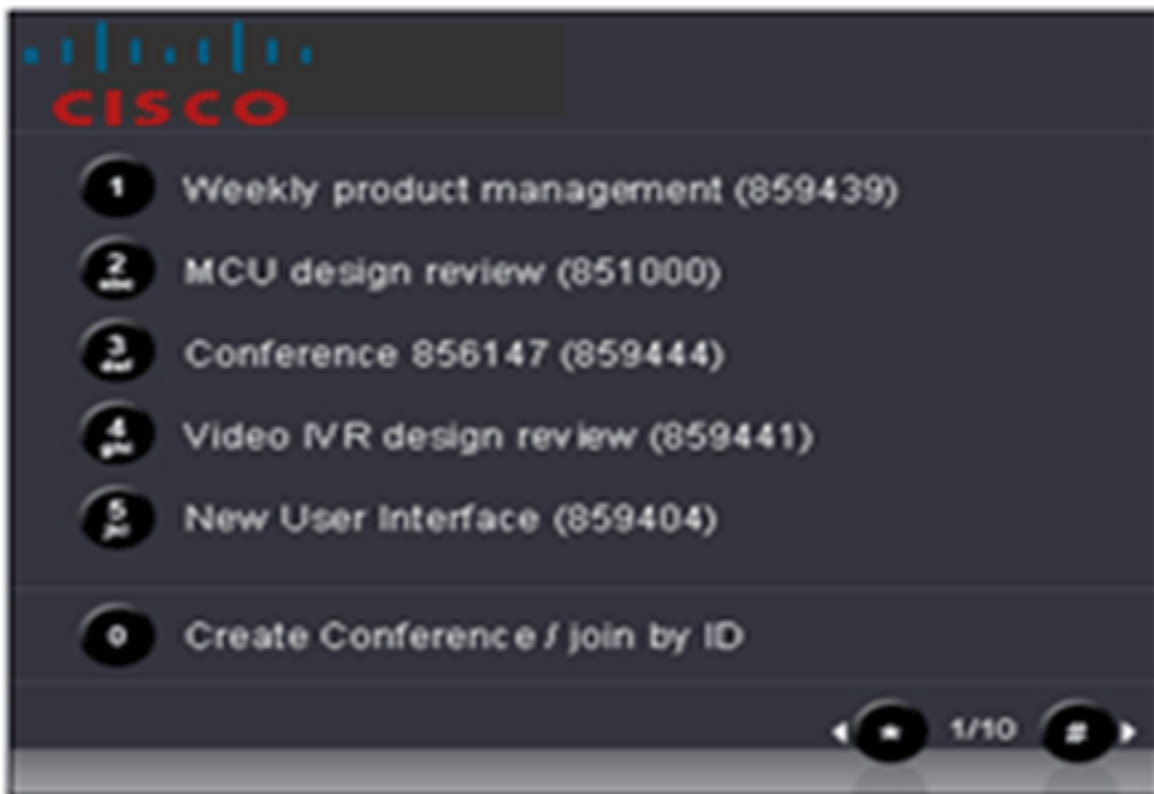
此镜像在Cisco Unified视频会议管理器的资源管理部分内显示验证Cisco IOS网守成功地添加。您能看到用172.16.1.100的IP地址列出的Cisco IOS H.323网守。



此镜像在显示对应于在多维数据集配置的空被叫号码。的e.164地址的Cisco Unified视频会议显示 Auto Attendant配置(1234567890)



此镜像显示什么Cisco IPVC视频IVR将退还到呼叫的视频端点。使用视频端点的遥控或键盘控制，用户通过(的DTMF选择在CUVC MCU被召开的视频会议在波段之内)并且加入适当的视频会议。



[故障排除](#)

目前没有针对此配置的故障排除信息。

[相关信息](#)

- [语音技术支持](#)
- [语音和统一通信产品支持](#)
- [Cisco IP 电话故障排除](#)
- [技术支持和文档 - Cisco Systems](#)