Elemento unificado de la frontera (CUBO) con el ejemplo unificado de la configuración de IVR de la Videoconferencia (CUVC)

Contenido

Introducción

La adopción de los comunicación mediante video basados en IP dentro de la empresa está bien en curso. En el entorno, el vídeo económicos de hoy del uso de los clientes más con frecuencia como herramienta para las comunicaciones de la intra-compañía con los beneficios mayores de esta adopción que es aumentos en la productividad del empleado y las eficacias operativas.

La mayoría de las redes basadas en IP de los comunicación mediante video de la empresa son hoy como las islas en relación con otras tales redes para empresas interconectadas usando una más vieja tecnología del Integrated Services Digital Network (ISDN). El ISDN es muy de uso general para toda la adicional-empresa o comunicación del adicional-campus con los otros sectores y, en algunos casos, incluso con las sucursales remotas dentro de la empresa sí mismo. Las ventajas de gran envergadura de los comunicación mediante video basados en IP se pueden realizar verdad con la conectividad del IP de punta a punta dentro o entre de las organizaciones para facilitar (B2B) las comunicaciones interempresariales. Esto requiere una transición del ISDN a las soluciones basadas en IP que atraviesan Internet en vez del PSTN, habilitando una opción convergida menos costosa para la intra-compañía y B2B las comunicaciones.

La transición al por mayor de los circuitos ISDN a las conexiones IP vía Internet no es una empresa trivial. Los circuitos ISDN, y los gatewayes video que atan el ISDN en los comunicación mediante video basados en IP mundo, son soluciones extensamente desplegadas, consagradas y de confianza. A pesar de las limitaciones en los servicios de comunicación mediante video serviciales de la última generación, el ISDN todavía fija el estándar contra el cual se miden las nuevas soluciones al tomar en la Seguridad, la aislamiento, la factura, y la demarcación de la

consideración. Las nuevas soluciones deben ofrecer las garantías similares del servicio-nivel para que las empresas y los proveedores de servicio los consideren como alternativa viable. Las empresas necesitan así una manera de mantener todas las ventajas asociadas al ISDN mientras que explotan las eficacias de extender los comunicación mediante video basados en IP más allá de la empresa.

Este ejemplo de configuración resalta las características del Cisco Unified Border Element (CUBO) e ilustra específicamente cómo el CUBO soporta la capacidad para un punto final que resida en alguna parte en Internet para marcar vía una dirección IP a una unidad de control multipunto (MCU) o al punto final que estén detrás de un escurdo de protección corporativo. Estas funciones muestran la característica de la *invalidación del nulo-llamar-número* disponible en la versión 12.4(22)YB del CUBO 1.3 y la funcionalidad IVR disponible en la versión 5.6 de la Videoconferencia unificada Cisco (CUVC) MCU. Este documento contiene las recomendaciones para la configuración y los puntos de partida posibles para las empresas que se embarcan en esta evolución.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento básico de cómo configurar y utilizar la voz del Cisco IOS (tal como dial peer)
- Conocimiento básico de cómo configurar y utilizar el CUBO
- Comprensión básica de cómo los Firewall trabajan

Componentes Utilizados

La información en este documento se basa encendido:

- Cisco Unified Border Element y Cisco IOS Gatekeeper que se ejecuta en un Cisco 2800 Router y utiliza el Cisco IOS Release 12.4.22(YB) o el Cisco IOS Release 15.0.1M
- Solución de la videoconferencia 3545 IP de Cisco que ejecuta la versión de software 5.6 o más adelante

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

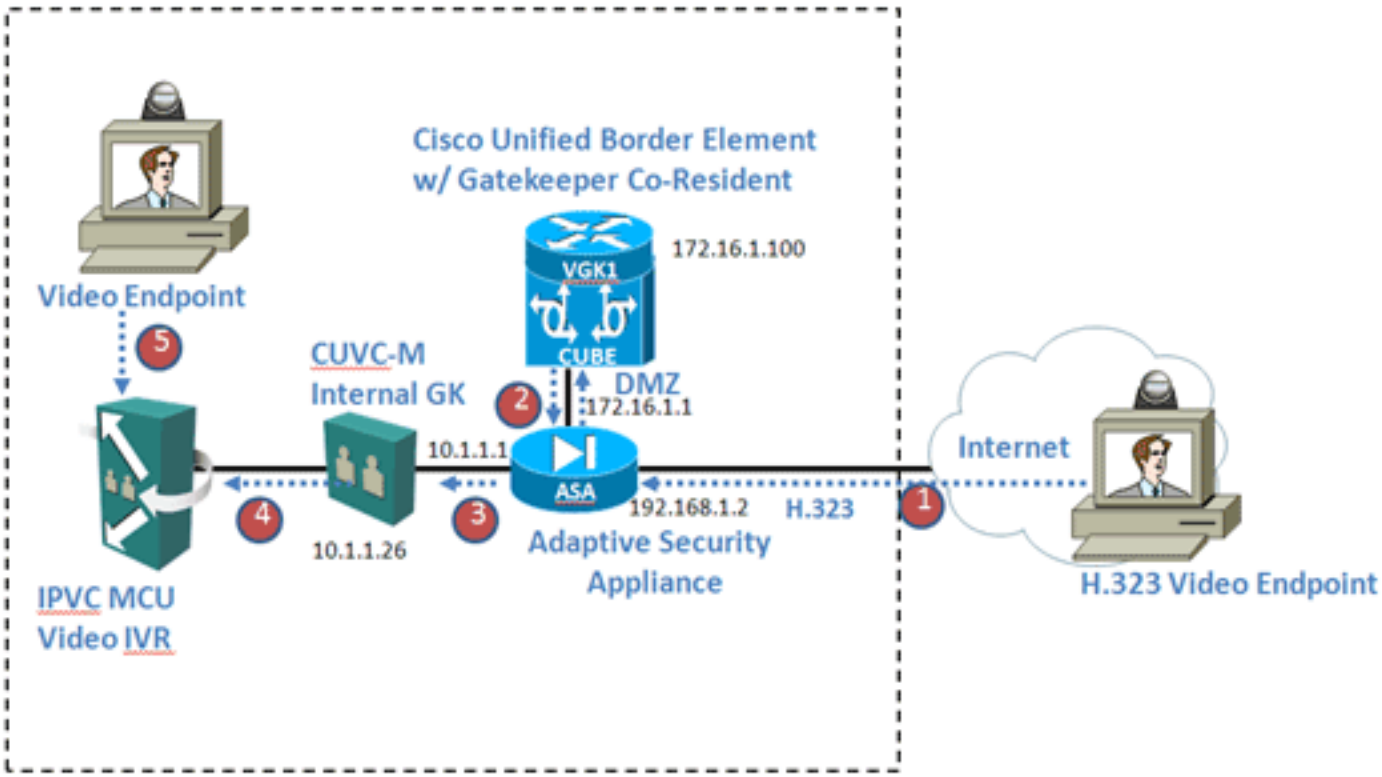
Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la herramienta Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

Este diagrama muestra a CUBO los puntos finales externos que marcan con seguridad en la red del cliente vía una dirección IP interna del punto final.



Flujo de llamada del diagrama

1. Un punto final externo en Internet marca a un IP Address público del CUBO (192.168.1.2) para unirse a un Video conferencia. que resida en una unidad de control multipunto interna de Cisco (MCU). Los mensajes de configuración de llamada de H.323 llegan el CUBO en virtud de un *agujerito* inicial para el puerto TCP 1720 configurado en el dispositivo de seguridad adaptante de Cisco (ASA) que es el Firewall que proporciona el límite de la Seguridad para la red. En este ejemplo, el CUBO tiene un IP Address privado así que la dirección enrutable apuntada por el punto final exterior es público el resultado de un NAT estático (traducción de dirección de red) realizado por el ASA.**Nota:** A título de ejemplo, Cisco utiliza solamente los espacios de IP Address privado en la documentación.
2. Puesto que el mensaje de CONFIGURACIÓN entrante no incluye los dígitos marcados usuales por los cuales el CUBO apuntaría normalmente la pierna siguiente de la llamada, el CUBO utiliza los dígitos (1234567890) configurados por el comando configuration de la **invalidación del nulo-llamar-número**. Usando este direccionamiento, los mensajes de configuración de llamada proceden hacia la red del cliente interno.
3. El ASA tiene dos agujeritos para soportar esta etapa de la llamada: uno para permitir el CUBO mire para arriba a la dirección deseada vía la característica interna del portero CUVC-M y uno para permitir que el mensaje setup resultante del CUBO consiga a CUVC-M establecer la llamada al MCU basado en el direccionamiento E.164 configurado en el dial peer en el CUBO. Usando la característica del examen de H.323 en el ASA, la señalización

y los media restantes fluyen TCP y las conexiones UDP se abren dinámicamente según la información espigada de la señalización de la configuración de la llamada.

4. El portero interno CUVC-M rutea la llamada al IPVC-MCU que incluye una nueva característica del vídeo IVR que presente un menú de opciones gráfico al usuario externo. Este menú es navegado ingresando los tonos DTMF vía la pista del dial o el Control remoto del punto final de llamada. El usuario final selecciona simplemente el ID de conferencia de la *opción de menú de la conferencia del unido* y después ingresa la contraseña necesaria si está configurado.
5. El punto final de video interno se une a la conferencia marcando el mismo ID de conferencia que el punto final externo.

Configuraciones

En este documento, se utilizan estas configuraciones:

- Ejemplo de configuración del CUBO
- Ejemplo de configuración ASA

Configuración del CUBO

```
!
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
```

Configuración ASA

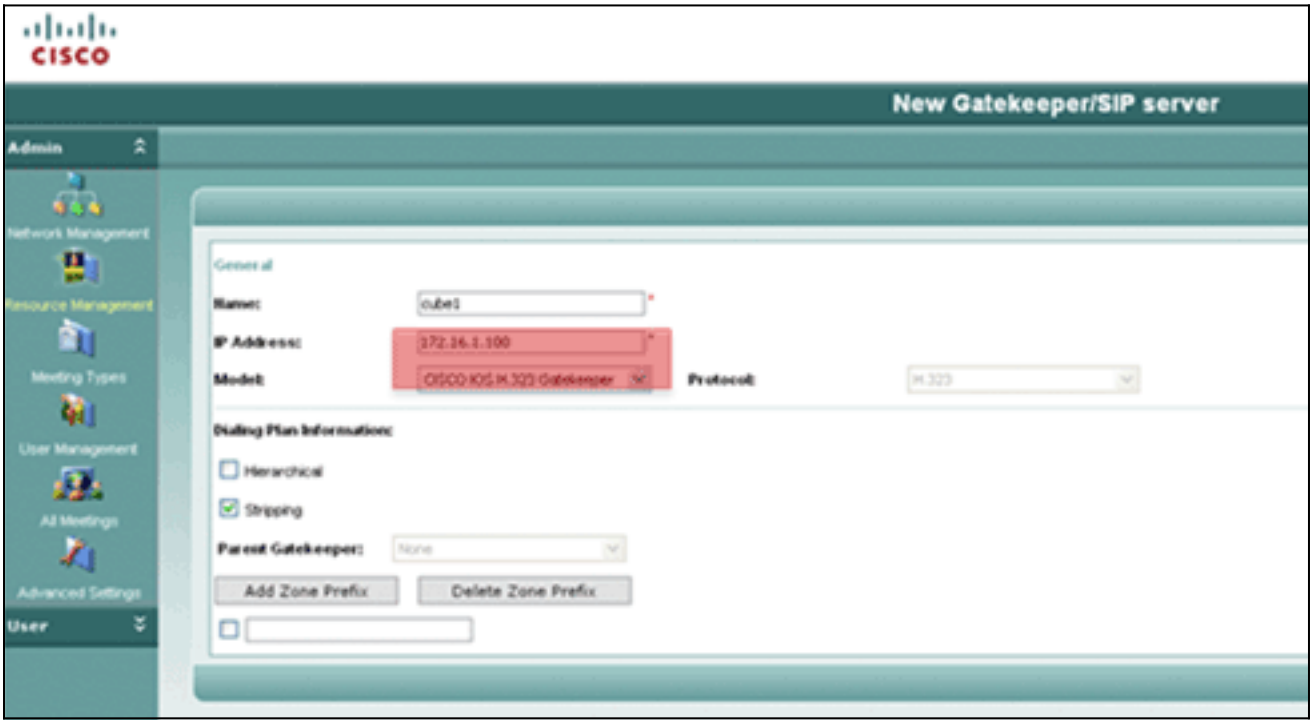
```
ASA Version 8.2(1)
!
!--- This is only a portion of the ASA config. !--- In a
typical production scenario, these commands would !---
be in addition to the current security policies
configured. ! interface Ethernet0/0 no nameif no
security-level no ip address ! interface Ethernet0/0.2
vlan 2 nameif 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
```

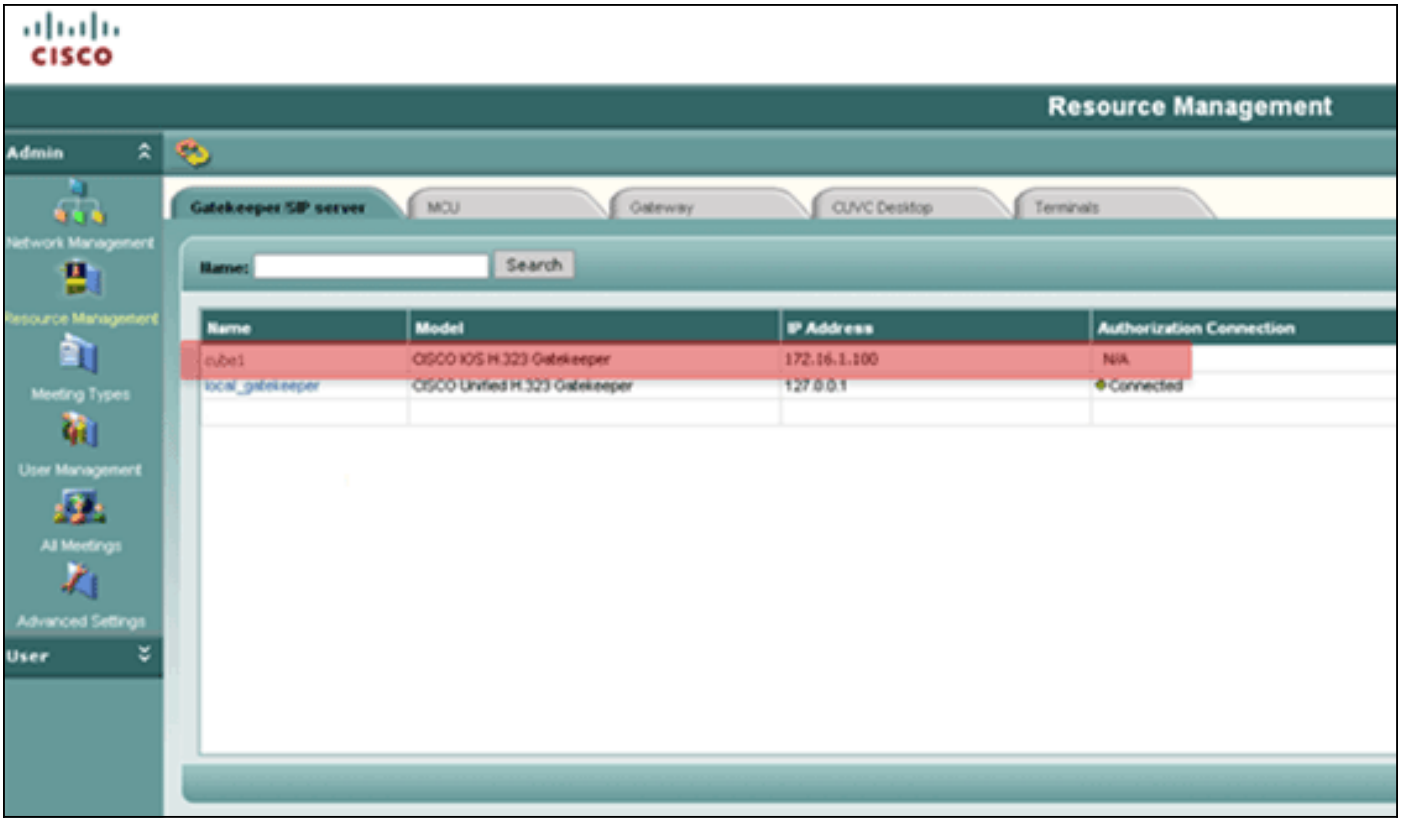
Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

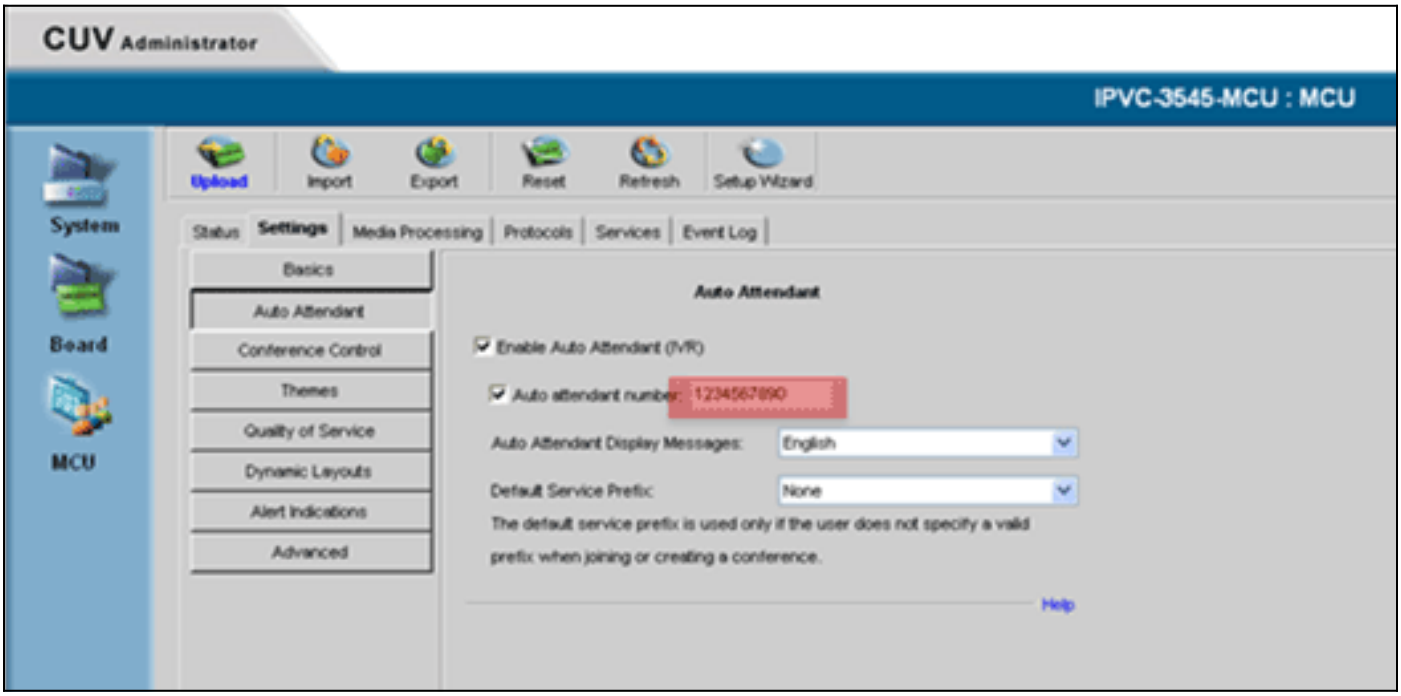
Esta imagen muestra al Cisco IOS Gatekeeper que es agregado al Cisco Unified Videoconferencing Manager. El modelo del Cisco IOS Gatekeeper se selecciona en la lista desplegable.



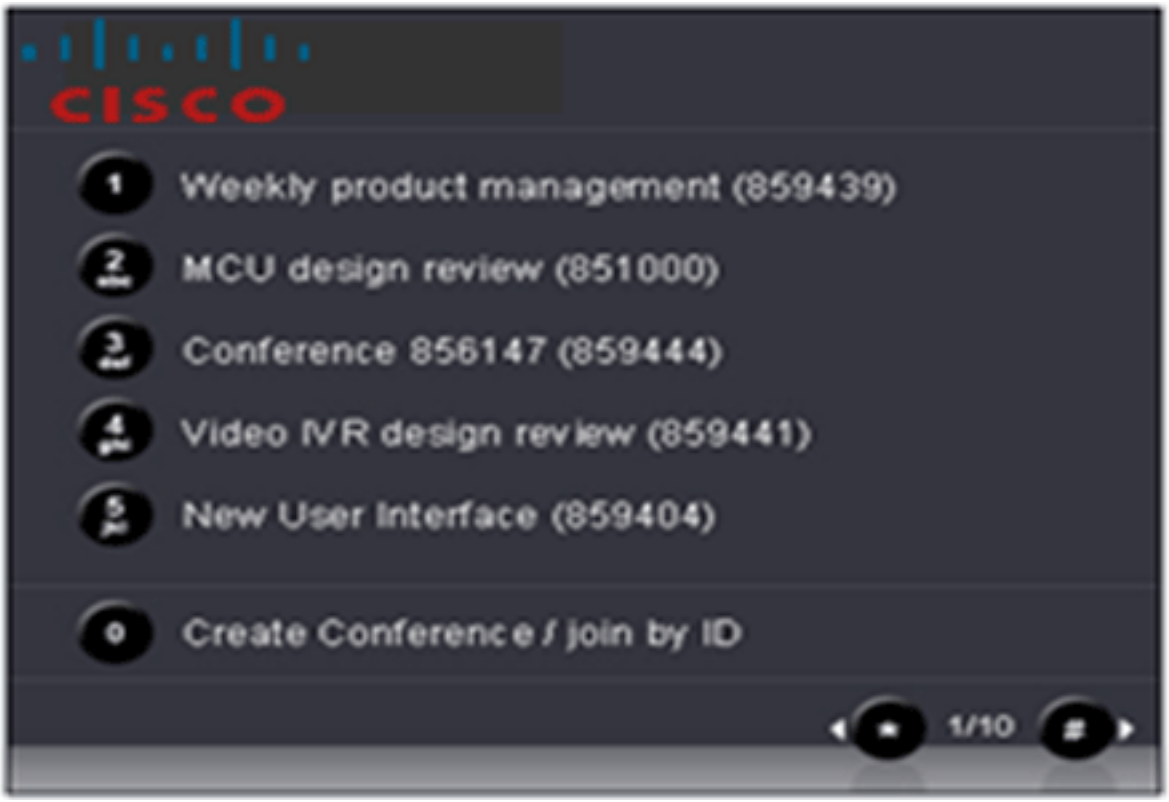
Esta imagen muestra que la verificación dentro de la sección de administración de recursos de Cisco unificó al administrador de la videoconferencia que agregaron al Cisco IOS Gatekeeper con éxito. Aquí usted puede ver al portero de H.323 del Cisco IOS enumerado con la dirección IP de 172.16.1.100.



Esta imagen muestra la configuración del Auto Attendant en la videoconferencia unificada Cisco que visualiza el direccionamiento e.164 (1234567890) que corresponden a la falta de información número al que se llamó configurada en el CUBO.



Este las imágenes muestran lo que devolverá el vídeo IVR de Cisco IPVC al punto final de video de llamada. Usando el Control remoto o el control del telclado numérico del punto final de video, el usuario elige una reunión video vía el DTMF (en-banda) que se recibe en el CUVC MCU y se une a la reunión video apropiada.



Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Soporte de tecnología de voz
- Soporte de Productos de Voice and Unified Communications
- Troubleshooting de Cisco IP Telephony
- Soporte Técnico y Documentación - Cisco Systems