

# Configuración y resolución de problemas de un ATA 186 con el IOS de Cisco Gatekeepers

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Diagrama de la red](#)

[Registro de ATA 186 con el gatekeeper](#)

[Adición de seguridad](#)

[Autenticación del punto final en el control de acceso con una ID de H.323.](#)

[Autenticar el punto final en el control de acceso con una dirección E.164](#)

[Autenticar el punto final en el control de acceso con una ID y contraseña H.323](#)

[Autentique el terminal en el gatekeeper con una dirección E.164 y una contraseña](#)

[Autenticar el punto final en el control de acceso con un ID H.323 y una contraseña mediante el separador](#)

[Verificación](#)

[Troubleshoot](#)

[Solución de problemas del control de acceso](#)

[Solución de problemas de ATA 186](#)

[Depuraciones de muestra para llamadas realizadas desde ATA 186](#)

[Información Relacionada](#)

## [Introducción](#)

El adaptador telefónico analógico Cisco (ATA) 186 es un adaptador de microteléfono a Ethernet que permite conectar teléfonos analógicos estándar a redes de telefonía IP. El ATA 186 tiene dos puertos de voz que solo pueden soportar teléfonos analógicos antiguos de marcación por tonos. A diferencia de los puertos normales de la Estación de Intercambio Remoto (FXS), estos no se pueden interconectar con una central telefónica privada (PBX) porque el ATA 186 no puede enviar dígitos en estos puertos. Con esta configuración, puede utilizar ambos puertos de voz con diferentes direcciones E.164 en cada uno.

## [Prerequisites](#)

## [Requirements](#)

Este documento asume que el lector está familiarizado con el contenido del documento

## [Configuración básica de Cisco ATA 186.](#)

Esta configuración requiere que el ATA 186 esté en la versión 2.0 o posterior, usando el conjunto de características H.323.

Asegúrese de que haya conectividad IP entre los dispositivos ATA 186, gateway y gatekeeper. Además, asegúrese de que el ATA 186 esté accesible a través del método del servidor web para una configuración posterior.

## [Componentes Utilizados](#)

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- ATA 186 con versión 2.12
- Cisco 3640 con Cisco IOS® Software Release 12.1 como gateway
- Cisco 2600 con Cisco IOS Software Release 12.2 como gatekeeper

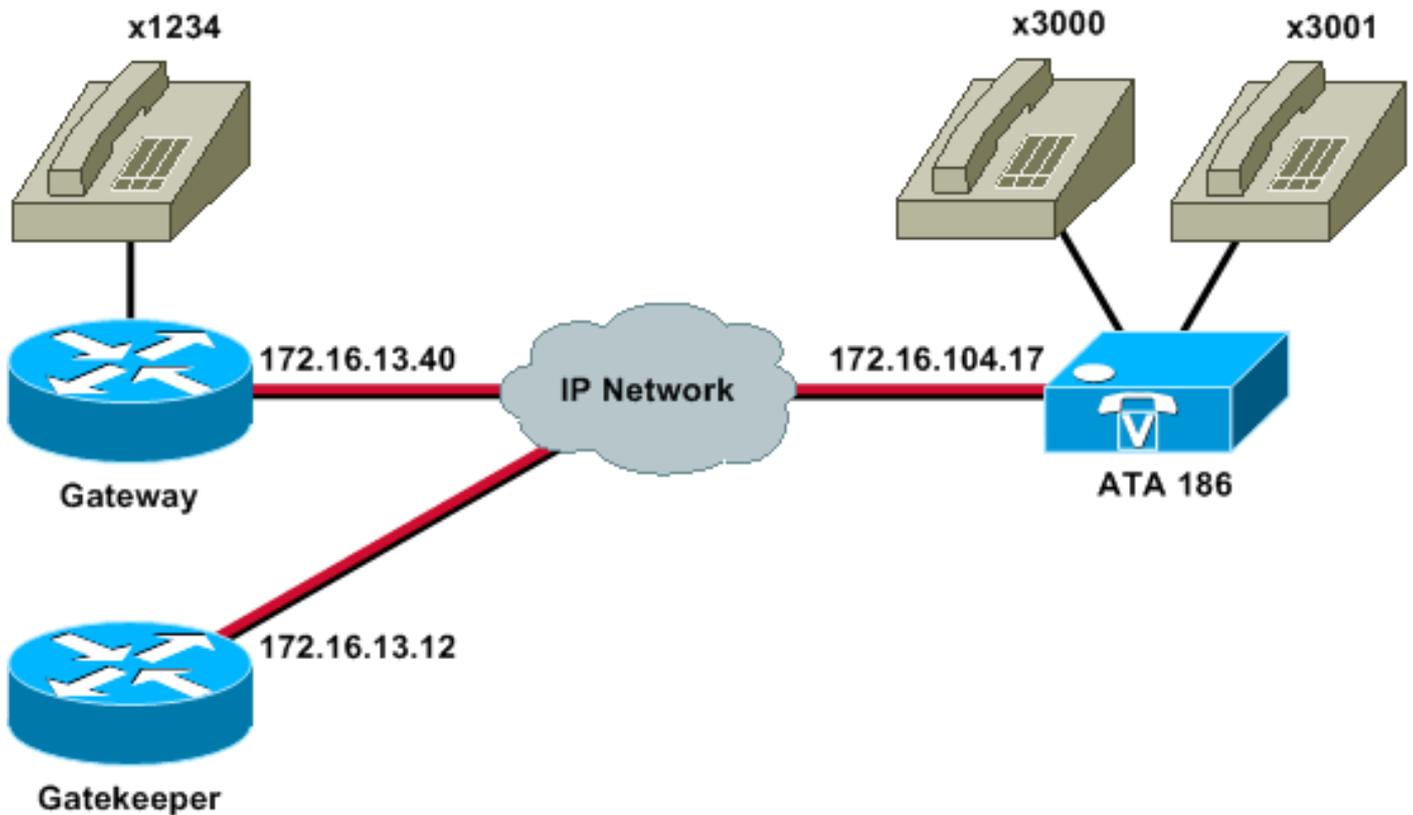
La información que se presenta en este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. All of the devices used in this document started with a cleared (default) configuration. Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener un comando antes de ejecutarlo.

## [Convenciones](#)

For more information on document conventions, refer to the [Cisco Technical Tips Conventions](#).

## [Diagrama de la red](#)

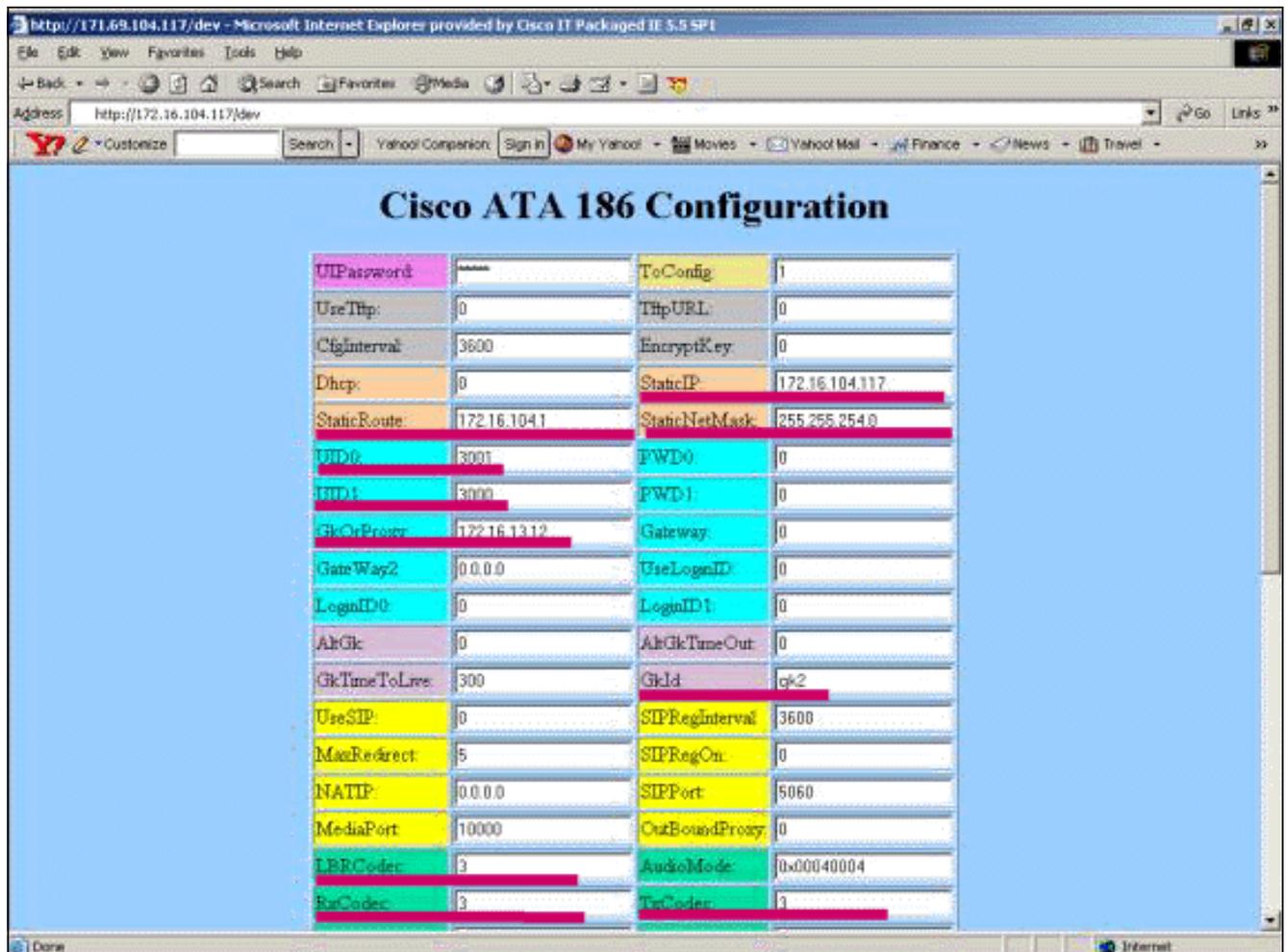
En este documento, se utiliza esta configuración de red:



## [Registro de ATA 186 con el gatekeeper](#)

Siga estas instrucciones para registrar el ATA 186 con el gatekeeper.

1. En un campo Dirección o Ubicación del navegador web, escriba la URL **http://ip\_address\_of\_ata/dev** para acceder a la pantalla de configuración ATA 186, donde **ip\_address\_of\_ata** es la dirección IP del ATA 186 que está registrando. En este ejemplo, la URL es **http://172.16.104.117/dev**. Aparece la ventana Cisco ATA 186 Configuration. **.Nota:** Los campos subrayados son los parámetros configurados relevantes para este escenario.



El direccionamiento IP se puede realizar estática o dinámicamente, como se explica en el documento [Configuración básica de Cisco ATA 186](#). En la pantalla anterior, se utiliza la dirección IP estática.

- En la ventana Cisco ATA 186 Configuration, configure estos campos: UID0 y UID1: configure las direcciones E.164 de los puertos de voz 0 y 1. Ambos puertos de voz no pueden tener la misma dirección E.164, ya que el ATA 186 no puede cazar si uno de los puertos está ocupado. Si a ambos puertos de voz se les asigna la misma dirección E.164, la llamada siempre se enviará al primer puerto de voz. Si este puerto está ocupado, la señal de ocupado se envía a la persona que llama. RxCodec y TxCodec: configure la ID de códec. G.723.1: codec ID 0. G.711a: ID de códec 1. G.711u: codec ID 2. G.729a: codec ID 3. En la configuración que se muestra a continuación, el códec G.729a se utiliza en el ATA 186 y en el gateway. LBRCodec: configure como 0 o 3, en función del códec seleccionado. LBR es 0: el códec G.723.1 está disponible para ambos puertos FXS en cualquier momento. Cada línea puede mantener dos llamadas G.723.1 en un estado de no conferencia. Por lo tanto, se pueden mantener hasta cuatro llamadas G.723.1 en el Cisco ATA 186. Un ejemplo es llamada en espera. LBR es 3: G.729a está disponible para uno de los dos puertos FXS por orden de llegada. Si la gateway de Cisco IOS se configura con el códec G.729 predeterminado, sólo se puede utilizar un puerto ATA 186. Para evitar que falle la segunda llamada, configure una clase de códec de voz en el gateway para negociar la segunda llamada usando un códec G.711. Para obtener información detallada, consulte la sección [Negociación de Códecs](#) de [Comprensión de Códecs](#): documento [Complejidad, Soporte de Hardware, MOS y Negociación](#). GkOrProxy: configure la dirección IP del gatekeeper. Una vez hecho esto, todo lo que se marca desde los puertos de voz ATA 186 se envía al gatekeeper.

3. Haga clic en el botón **Aplicar** y, a continuación, vuelva a cargar la página. El ATA 186 tarda 10 segundos en reconfigurarse.

Estos ejemplos son configuraciones relevantes para el gatekeeper y la gateway de Cisco IOS:

### Gatekeeper 2610

```
interface Ethernet0/0
 ip address 172.16.13.12 255.255.255.224
 half-duplex
 h323 interface
 h323 h323-id pro
 h323 gatekeeper ipaddress 172.16.13.12
 h323 t120 bypass
 !
dial-peer cor custom
 !
 !
 !
gatekeeper
 zone local gk2 cisco.com 172.16.13.12
no shutdown
 !
```

### Gateway 3640

```
interface Ethernet0/0
 ip address 172.16.13.40 255.255.255.224
 half-duplex
 !
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.13.33
ip http server
 !
 !
 !
voice-port 3/0/0
 !
voice-port 3/0/1
 !
dial-peer cor custom
 !
 !
 !
dial-peer voice 1 pots
 destination-pattern 34
 port 3/0/0
 !
dial-peer voice 2 pots
 destination-pattern 45
 port 3/0/1
 !
dial-peer voice 100 pots
 destination-pattern 1234
 port 3/0/0
 !
dial-peer voice 3000 voip
 destination-pattern 300.
 session target ras
!--- Dial-peer to send the calls to ATA. !
```

## Adición de seguridad

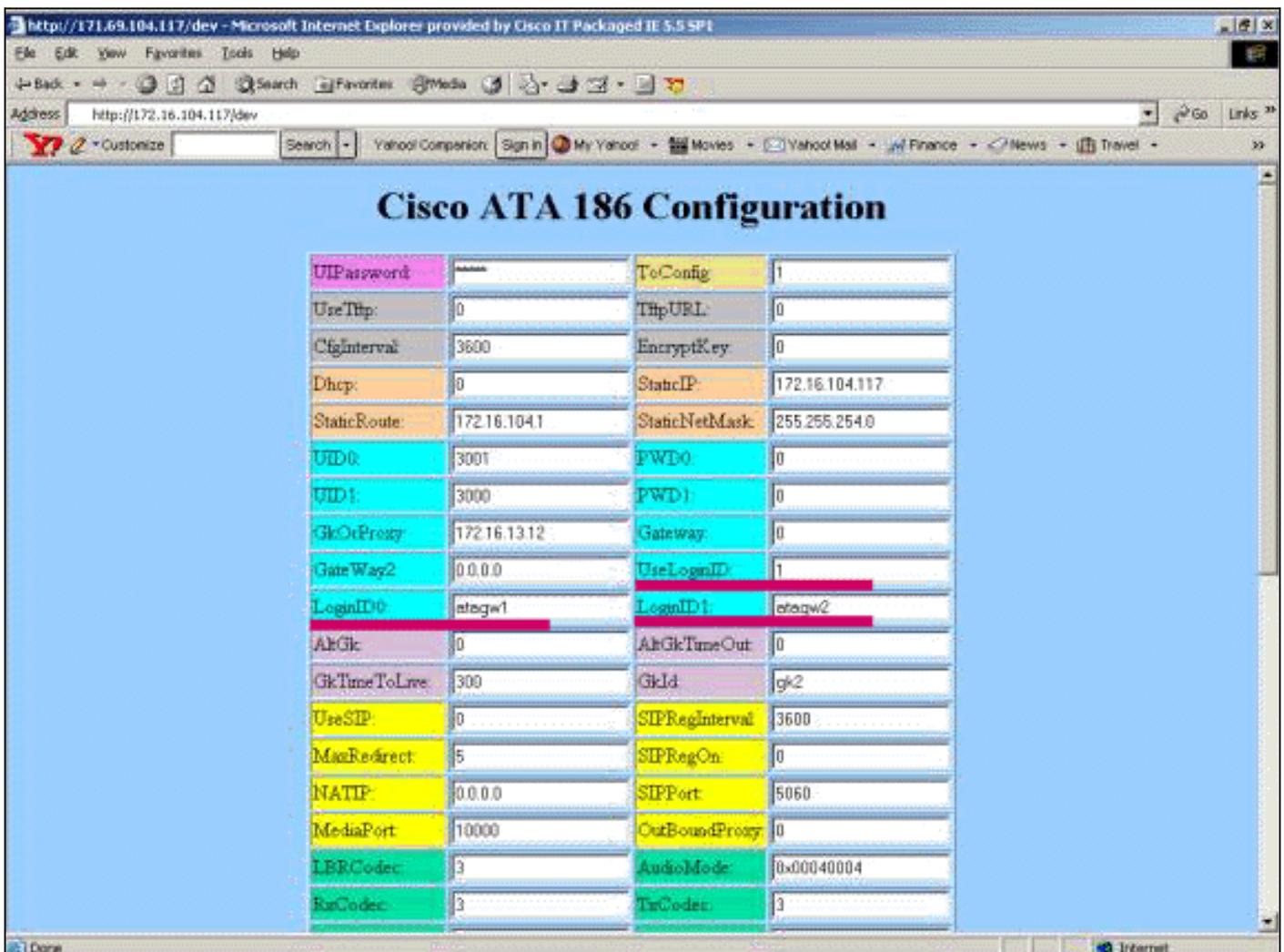
A partir de la versión 2.12 del software ATA, las opciones de esta sección están disponibles para agregar seguridad.

### Autenticación del punto final en el control de acceso con una ID de H.323.

Siga estos pasos para configurar el ATA 186 para registrarse con el ID H.323:

1. Establezca el campo AutMethod en 0 (el valor predeterminado es 1). El valor hexadecimal que se va a configurar para este campo es 0x0.
2. Establezca el campo UseLoginID en 1.
3. Configure LoginID0 e LoginID1, con los ID H.323 para ATA 186. El ATA 186 se registra como dos terminales H.323 diferentes, uno para cada puerto.

Este es un ejemplo de configuración de trabajo para el gatekeeper cuando se usa ATA con el método de autenticación de ID H.323:



#### Gatekeeper 2610

```
aaa authentication login default local
aaa authentication login cisco none
aaa authentication login h323 local
aaa session-id common
```

```
enable password ww
!
username atagw1
!--- Same as the LoginID0 and LoginID1 fields. username
atagw2 username 3640
!--- Same as the H.323 ID configured on the gateway. !
gatekeeper zone local gk2 cisco.com 172.16.13.12
security any
!--- Register after the H.323 ID or E.164 address is
authenticated. no shutdown !
```

## [Autenticar el punto final en el control de acceso con una dirección E.164](#)

Siga estos pasos para configurar el ATA 186 para registrarse con la dirección E.164:

1. Establezca el campo AutMethod en 0 (el valor predeterminado es 1).El valor hexadecimal que se va a configurar para este campo es 0x0.
2. Establezca el campo UseLoginID en 0.El ATA utiliza los campos UID0 y UID1 para ser autenticado por el gatekeeper.

Este es un ejemplo de configuración de funcionamiento para el gatekeeper y la gateway cuando se usa ATA con el método de autenticación de ID E.164:

### **Gatekeeper 2610**

```
aaa authentication login default local
aaa authentication login cisco none
aaa authentication login h323 local
aaa session-id common
enable password ww
!
username 3001
!--- Same as the UID0. username 3000
!--- Same as the UID1. ! gatekeeper zone local gk2
cisco.com 172.16.13.12 security any
!--- Register after the H.323 ID or E.164 address is
authenticated. no shutdown !
```

## [Autenticar el punto final en el control de acceso con una ID y contraseña H.323](#)

Siga estos pasos para configurar el ATA 186 para registrarse con el ID y la contraseña H.323:

1. Establezca el campo AutMethod en 1 (el valor predeterminado es 1).El valor hexadecimal que se va a configurar para este campo es 0x1. Este campo está configurado para indicar que el ATA busca ahora la contraseña.
2. Establezca el campo UseLoginID en 1.
3. Configure LoginID0 e LoginID1, con los ID H.323 para ATA 186.El ATA 186 se registra como dos terminales H.323 diferentes, uno para cada puerto.
4. Configure PWD0 y PWD1 con la contraseña para cada puerto.**Nota:** El ATA utiliza la contraseña para generar el token. Este token se envía al gatekeeper para la autenticación.
5. Configure NTP con la dirección IP del servidor del protocolo de tiempo de red (NTP).El gatekeeper y el ATA deben tener relojes sincronizados con el mismo servidor NTP.

**Nota:** La marca de tiempo se utiliza para la generación de token. Para obtener más información, consulte la [Guía de solución de problemas de seguridad de puerta de enlace al control de acceso](#)

[\(H.235\) y de control de acceso al control de acceso \(IZCT\).](#)

Este es un ejemplo de configuración de funcionamiento para el gatekeeper y la gateway cuando se usa ATA con el método de autenticación de ID y contraseña H.323:

```
Gatekeeper 2610

aaa authentication login default local
aaa authentication login cisco none
aaa authentication login h323 local
aaa session-id common
enable password ww
!
username atagw1 password cisco
!--- Same as the LoginID0 and PWD0 fields. username
atagw2 password cisco
!--- Same as the LoginID1 and PWD1 fields. ! gatekeeper
zone local gk2 cisco.com 172.16.13.12 security token
required-for registration
!--- Register after the H.323 ID or E.164 address and
token is authenticated. no shutdown !
```

**Nota:** Para obtener más información sobre la seguridad del control de acceso, consulte la [Guía de solución de problemas de seguridad de puerta de enlace al control de acceso \(H.235\) y de control de acceso al control de acceso \(IZCT\).](#)

## [Autentique el terminal en el gatekeeper con una dirección E.164 y una contraseña](#)

Siga estos pasos para configurar el ATA 186 para que se registre con el ID y la contraseña E.164:

1. Establezca el campo AutMethod en 1 (el valor predeterminado es 1).El valor hexadecimal que se va a configurar para este campo es 0x0. Este campo está configurado para indicar que el ATA buscará la contraseña.
2. Establezca el campo UseLoginID en 0.
3. Configure UID0 y UID1 con los ID E.164 para el ATA 186.El ATA 186 se registra como dos terminales H.323 diferentes, uno para cada puerto.
4. Configure PWD0 y PWD1 con la contraseña para cada puerto.**Nota:** El ATA utiliza la contraseña para generar el token. Este token se envía al gatekeeper para la autenticación.
5. Configure NTP con la dirección IP del servidor NTP.El gatekeeper y el ATA deben tener relojes sincronizados con el mismo servidor NTP.

**Nota:** La marca de tiempo se utiliza para la generación de token. Para obtener más información, consulte la [Guía de solución de problemas de seguridad de puerta de enlace al control de acceso \(H.235\) y de control de acceso al control de acceso \(IZCT\).](#)

Este es un ejemplo de configuración en funcionamiento para el gatekeeper y la gateway cuando se usa ATA con el método de autenticación de ID y contraseña E.164:

```
Gatekeeper 2610

aaa authentication login default local
aaa authentication login cisco none
aaa authentication login h323 local
aaa session-id common
```

```
enable password ww
!
username 3001 password cisco
!--- Same as the UID0 and PWD0 fields. username 3000
password cisco

!--- Same as the UID1 and PWD1 fields. ! gatekeeper zone
local gk2 cisco.com 172.16.13.12 security token
required-for registration
!--- Register after the H.323 ID or E.164 address and
token is authenticated. no shutdown !
```

**Nota:** Para obtener más información sobre la seguridad del control de acceso, consulte la [Guía de solución de problemas de seguridad de puerta de enlace al control de acceso \(H.235\)](#) y de control de acceso al control de acceso (IZCT).

## [Autenticar el punto final en el control de acceso con un ID H.323 y una contraseña mediante el separador](#)

Siga estos pasos para configurar el ATA 186 para registrarse con el ID y la contraseña H.323:

1. Establezca el campo AutMethod en 1 (el valor predeterminado es 1). El valor hexadecimal configurado para este campo es 0x1. Este campo está configurado para indicar que el ATA busca ahora la contraseña.
2. Establezca el campo UseLoginID en 1.
3. Configure LoginID0 e LoginID1 con los ID H.323, seguido del separador y la contraseña para el ATA 186. Por ejemplo, LoginID0 es **atagw1=cisco**. El ATA 186 se registra como dos terminales H.323 diferentes, uno para cada puerto. **Nota:** El ATA utiliza la contraseña para generar el token. Este token se envía al gatekeeper para la autenticación.
4. Configure NTPIP con la dirección IP del servidor NTP. El gatekeeper y el ATA deben tener relojes sincronizados con el mismo servidor NTP.

**Nota:** La marca de tiempo se utiliza para la generación de token. Para obtener más información, consulte la [Guía de solución de problemas de seguridad de puerta de enlace al control de acceso \(H.235\)](#) y de control de acceso al control de acceso (IZCT).

Este es un ejemplo de configuración de funcionamiento para el gatekeeper y la gateway cuando se usa ATA con el método de autenticación de ID y contraseña H.323 usando un separador:

### Gatekeeper 2610

```
aaa authentication login default local
aaa authentication login cisco none
aaa authentication login h323 local
aaa session-id common
enable password ww
!
username atagw1 password cisco
!--- Same as the LoginID0 and PWD0 fields. username
atagw2 password cisco
!--- Same as the LoginID1 and PWD1 fields. ! gatekeeper
zone local gk2 cisco.com 172.16.13.12 security h323-id
security password separator =
!--- Register after the H.323 ID or E.164 address and
token is authenticated. no shutdown !
```

**Nota:** Para obtener más información sobre la seguridad del control de acceso, consulte la [Guía de solución de problemas de seguridad de puerta de enlace al control de acceso \(H.235\) y de control de acceso al control de acceso \(IZCT\)](#).

## Verificación

El ejemplo de esta sección muestra el registro del punto final del gatekeeper.

Para verificar la configuración, ejecute el comando **show gatekeeper endpoint**.

```
GATEKEEPER_ENDPOINT
REGISTRATION

CallSignalAddr  Port  RASignalAddr  Port  Zone Name  Type  Flags
-----
172.16.13.40    1720  172.16.13.40  50923  gk2        VOIP-GW  E164-ID: 1234
                                           H323-ID: 3640
172.16.13.43    1720  172.16.13.43  58400  gk2        VOIP-GW  H323-ID: 3660-2
172.16.104.117  1720  172.69.85.90  1719   gk2        TERM     E164-ID: 3000
172.16.104.117  1721  172.69.85.90  1739   gk2        TERM     E164-ID: 3001
Total number of active registrations=3
```

**Nota:** El ATA 186 se registra como terminal H.323 (**TERM**) y no como gateway H.323. Esto se hace deliberadamente para que sólo se le envíen las llamadas destinadas al ATA 186.

**Nota:** No puede tener ninguna dirección en el campo de gateway ATA. No puede configurar el ATA 186 para que funcione tanto con el gatekeeper como con el gateway.

## Troubleshoot

Esta sección proporciona la información para resolver problemas en su configuración.

El ATA 186 no proporciona tono de marcado si no se registra correctamente con el gatekeeper. Si el ATA 186 no se está registrando con el gatekeeper, verifique estos elementos:

- La conectividad IP existe entre el ATA 186 y el gatekeeper.
- Los campos ATA 186 UID0 y UID1 están configurados correctamente. Si los campos UID están configurados en 0, el ATA 186 no intenta registrarse con el gatekeeper. Como mínimo, el campo UID0 debe ser un valor distinto de cero, para que el ATA 186 inicie el proceso de registro. Si ambos puertos ATA 186 (UID0 y UID1) tienen direcciones E.164 distintas de cero, el ATA 186 intenta registrarse con ambos puertos. El ATA 186 no proporciona tono de marcado, incluso si uno de los puertos no puede registrarse.
- El gatekeeper está configurado correctamente. Si el gatekeeper está configurado con un prefijo de zona local, se debe incluir la dirección E.164 del ATA 186. Si se configura la seguridad en el gatekeeper, el ATA 186 debe configurarse en consecuencia.

Además, verifique que el campo UseSIP esté configurado en 0. Esto es necesario para configurar el ATA 186 en el modo H.323. Si el campo UseSIP se establece en 1, ATA 186 no envía la solicitud de registro al gatekeeper.

## Solución de problemas del control de acceso

Cuando se configura la seguridad, ejecute el comando [debug aaa authentication](#).

Si no se configura ninguna seguridad, ejecute el comando [debug ras](#).

**Nota:** El ATA 186 se registra por separado para los dos puertos de voz. El ATA 186, por lo tanto, se autentica dos veces como diferentes terminales H.323, como se muestra en este debug:

```
4w4d: AAA/AUTHEN/CONT (3800768902): continue_login (user='atagw1')
4w4d: AAA/AUTHEN (3800768902): status = GETPASS
4w4d: AAA/AUTHEN/CONT (3800768902): Method=LOCAL
4w4d: AAA/AUTHEN (3800768902): status = PASS
4w4d: AAA: parse name=<no string> idb type=-1 tty=-1
4w4d: AAA/MEMORY: create_user (0x83149EFC) user='atagw2'ruser='NULL' port='NULL'
rem_addr='NULL' authen_type=ASCII service=LOGIN priv=0 initial_task_id='0'
4w4d: AAA/AUTHEN/START (294225678): port='' list='h323' action=LOGIN service=LOGIN
4w4d: AAA/AUTHEN/START (294225678): found list h323
4w4d: AAA/AUTHEN/START (294225678): Method=LOCAL
4w4d: AAA/AUTHEN (294225678): status = GETPASS
4w4d: AAA/H323: Password:
4w4d: AAA/AUTHEN/CONT (294225678): continue_login (user='atagw2')
4w4d: AAA/AUTHEN (294225678): status = GETPASS
4w4d: AAA/AUTHEN/CONT (294225678): Method=LOCAL
4w4d: AAA/AUTHEN (294225678): status = PASS
4w4d: AAA: parse name=<no string> idb type=-1 tty=-1
4w4d: AAA/MEMORY: create_user (0x831910C0) user='3660' ruser='NULL' port='NULL'
rem_addr='NULL' authen_type=ASCII service=LOGIN priv=0 initial_task_id='0'
```

Para obtener más ejemplos de resolución de problemas, consulte [Resolución de problemas de registro del control de acceso](#).

## [Solución de problemas de ATA 186](#)

Cuando trabaja con gatekeepers y gateways de terceros, la herramienta de resolución de problemas del ATA 186 es muy útil. Para habilitar la herramienta de resolución de problemas ATA 186, siga estos pasos:

1. En el campo ATA Nprintf, configure la dirección IP del PC que se encuentra en la misma subred que el ATA 186.
2. El puerto especificado después de la dirección debe ser 9001.
3. En el mensaje DOS del equipo, ejecute el programa **preserv.exe**.

Puede descargar el programa preserv.exe del [Centro de Software de Cisco](#) (sólo clientes registrados).

El programa preserv.exe se incluye en el último archivo ZIP de la versión de software ATA 186.

## [Depuraciones de muestra para llamadas realizadas desde ATA 186](#)

```
D:\Documents and Settings\sshafiqu\My Documents\voice\ata>prserv.exe
```

```
GK<-1: KPA-RRQ:300 sec
```

```
GK->1: RCF:TTL 300
```

```
!--- ATA was reset after the gatekeeper configuration was added. WStop:0 Wed Feb 06 19:06:54
2002 Hello from 171.69.85.90(0) Build 1109a: v2.12 ata186 Successfully Registered with the
Gatekeeper GK zone<gk2>172.16.13.12: 3000 GK zone:gk2 0x13e138 delayed RRQ: 48 ticks: 300 GK
zone<gk2>172.16.13.12: 3001 GK zone:gk2 0x141e58 delayed RRQ: 56 ticks: 300 BMK : gk2 GK<-1:
```

```

KPA-RRQ:300 sec BMK : gk2 GK->0: KPA-RRQ:300 sec GK->1: RCF:TTL 300 GK->0: RCF:TTL 300 SCC->(0
0) <cmd 0> 3000 active @0xab45555a (GK @0xac100d0c) !--- Call made from voice port 0. [0]DTMF 1
[0]DTMF 2 [0]DTMF 3 [0]DTMF 4 [0]DTMF # Calling 1234 SCC->(0 0) <cmd 16> CLIP\ \SCC->(0 0) <cmd
2> \<0 0> dial<1234> GK->0: ARQ: 0
GK->0: ACF:0:direct call
IRR in 240 sec
CallRasCallBack: 1 33e15eb 33e206b 33e39b0
Connect to <0xac100d28 1720>>..
>>>>>>> TX CALLER ID : 0x1          0x80 6
Q931->0:Setup:CRV 25006
Q931->0:Proceeding
Connect H245...
H245 TCP conn ac100d28 11006
CESE/MSDSE start:<0 0 0 0>
capSize = 3
H245->0:Cese
RemoteInputCap <15 5>
RemoteInputCap <15 4>
RemoteInputCap <15 1>
RemoteInputCap <4 11>
MODE FRAME : 11 2
RemoteAudioCap <4 10>
Capability set accepted
H245->0:MSD: <rn tt> = <0x269c 60>
H245->0:CeseAck
H245->0:MsdAck
h323.c 1837: cstate : 3
->H245<0> OLC
H245->0:LcseOpen
set TX audio to G729/G729A 2 fpp
SetG723Mode: 2 0
H245->0:LcseOpen
H245->0:OLC mode 10
remote OpenLogicalReq G711/G729(10) : 2 fpp
OpenRtpRxPort(0,0x0,4000):14
RTP Rx Init: 0, 0
RTP->0:<0xab45555a 4000>
H245->0:LcseOpenAck
RTP->0:<0xac100d28 17304>
[0]Enable encoder 18
RTP TX[0]:SSRC_ID = 4af964c0
RTP Tx Init: 0, 0
[0]DPKT 1st: 861812319 861812079, pt 18
Enable LEC adapt [0]=1
H323Dispatcher : 3 3
[0]Received pi=8 in q931
Q931->0:Progress
Q931->0:Connect
SCC:ev=12[0:0] 3 0
Q931->0:ReleaseComplete: reason 16, tone = 13
H245->0:EndSessionCmd 1
0: Close RTPRX
write TCP err : 13 -33
[0:0]Rel LBRC Res
Q931<-*:ReleaseComplete
!--- ATA side hangs up the call. write TCP err : 12 -33 GK->0: DRQ:0
!--- Disconnect request sent by ATA. SCC:ev=13[0:0] 4 0 [0:0]SCC: Disconnected GK->0: DCF
!--- Disconnect confirm received. SCC->(0 0) <cmd 1> [0]MPT mode 0

```

## No hay ejemplo de depuración de ATA de tono de marcado

Ambos puertos de voz necesitan una dirección E.164 única; de lo contrario, el ATA recibe un Rechazo del gatekeeper. Durante este tiempo, verá el ATA 186 registrado con un puerto de voz

como terminal H.323, pero no habrá tono de marcado.

```
K<-0: GRQ  
BMK : gk2  
GK->0: GCF:GK@0xac100d0c-1719  
BMK : gk2  
Secured RRQ  
GK<-0: RRQ  
GK->0:RRJ: reason 4
```

## Información Relacionada

- [Configuración básica de Cisco ATA 186](#)
- [Configuración y solución de problemas del ATA 186 con un Gateway IOS de Cisco](#)
- [Gatekeeper de alto rendimiento de Cisco - Configuración del Gatekeeper](#)
- [Configuración de voz sobre IP](#)
- [Soporte de tecnología de voz](#)
- [Soporte de Productos de Voice and Unified Communications](#)
- [Troubleshooting de Cisco IP Telephony](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)