Instalación del teléfono H.323 de IP Office Platform

Versión 11.1 FP2
Edición 3
Noviembre de 2021

Notices

Aviso

Si bien se hicieron esfuerzos razonables para asegurar que la información contenida en este documento esté completa y sea exacta en el momento de su impresión, Avaya no se responsabiliza por los errores. Avaya se reserva el derecho de realizar cambios y correcciones a la información contenida en este documento sin la obligación de notificar a ninguna persona u organización sobre dichos cambios.

Exención de responsabilidad con respecto a la documentación

“Documentación” hace referencia a la información publicada en diversos medios, que puede incluir información del producto, instrucciones operativas y especificaciones de rendimiento, que se suelen poner a disposición de los usuarios de productos. La documentación no incluye material publicitario. Avaya no asume la responsabilidad por las modificaciones, adiciones o eliminaciones efectuadas en la versión original publicada de la Documentación, a menos que dichas modificaciones, adiciones o eliminaciones hayan sido realizadas por Avaya o expresamente a nombre de Avaya. El usuario final acuerda indemnizar y eximir de toda responsabilidad a Avaya, agentes de Avaya y empleados con respecto a todo reclamo, acción judicial, demanda y juicio que surgiere de o en relación con modificaciones, incorporaciones o eliminaciones posteriores en esta documentación realizadas por el usuario final.

Exención de responsabilidad con respecto a los vínculos

Avaya no asume la responsabilidad del contenido ni la fiabilidad de los enlaces a los sitios web incluidos en cualquier punto de este sitio o en la Documentación proporcionada por Avaya. Avaya no es responsable de la confiabilidad de ninguna información, instrucción ni contenido proporcionado en estos sitios y no necesariamente aprueba los productos, los servicios o la información descritos u ofrecidos por los mismos. Avaya no garantiza que estos vínculos funcionarán todo el tiempo ni tiene control de la disponibilidad de las páginas vinculadas.

Garantía

Avaya ofrece una garantía limitada para sus productos de hardware y software. Consulte su contrato de compraventa para establecer las condiciones de la garantía limitada. Además, el idioma de la garantía estándar de Avaya, así como la información relacionada con el soporte técnico para este producto durante el período de vigencia de la garantía, está disponible, tanto para los clientes como para otras personas interesadas, en el sitio web del Soporte Técnico de Avaya: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 o en el enlace “Warranty & Product Lifecycle” (Garantía y ciclo de vida del producto) o en el sitio web posterior designado por Avaya. Tenga en cuenta que si ha adquirido los productos de un Channel Partner de Avaya fuera de Estados Unidos y Canadá, la garantía es proporcionada por dicho Channel Partner y no por Avaya.

“**Servicio alojado**” significa una suscripción de servicio alojado por Avaya que Usted adquiere ya sea de Avaya o de un Channel Partner de Avaya (según corresponda) y que se describe detalladamente en SAS alojado u otra documentación de descripción del servicio sobre el servicio alojado correspondiente. Si compra una suscripción de servicio alojado, la garantía limitada anterior podría no ser aplicable, pero puede tener derecho a servicios de soporte técnico relacionados con el servicio alojado como se describe más adelante en los documentos de descripción del servicio para el servicio alojado correspondiente. Comuníquese con Avaya o el Channel Partner de Avaya (según corresponda) para obtener más información.

Servicio alojado

SE APLICA LO SIGUIENTE ÚNICAMENTE SI ADQUIERE UNA SUSCRIPCIÓN DE AVAYA A UN SERVICIO HOSPEDADO DE AVAYA O UN CHANNEL PARTNER DE AVAYA (SI CORRESPONDE), LOS TÉRMINOS DE USO PARA LOS SERVICIOS HOSPEDADOS ESTÁN DISPONIBLES EN EL SITIO WEB DE AVAYA HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO EN EL ENLACE “Avaya Terms of Use for Hosted Services” O EN LOS SITIOS FUTUROS QUE DESIGNE AVAYA, Y SE APLICAN A TODA PERSONA QUE TENGA ACCESO O USE EL SERVICIO HOSPEDADO. AL ACCEDER O USAR EL SERVICIO HOSPEDADO, O AL AUTORIZAR A TERCEROS A HACERLO, EN NOMBRE SUYO Y DE LA ENTIDAD PARA LA QUE ACCEDE O USA EL SERVICIO HOSPEDADO (EN ADELANTE, A LOS QUE SE HACE REFERENCIA INDISTINTAMENTE COMO “USTED” Y “USUARIO FINAL”), ACEPTA LOS TÉRMINOS DE USO. SI ACEPTA LOS TÉRMINOS DE USO EN NOMBRE DE UNA COMPAÑÍA U OTRA ENTIDAD LEGAL, USTED DECLARA QUE TIENE LA AUTORIDAD PARA VINCULAR A DICHA ENTIDAD CON LOS PRESENTES TÉRMINOS DE USO. SI NO CUENTA CON DICHA AUTORIDAD O SI NO ESTÁ DE ACUERDO CON LOS PRESENTES TÉRMINOS DE USO, NO DEBE ACCEDER NI USAR EL SERVICIO HOSPEDADO NI AUTORIZAR A TERCEROS A QUE ACCEDAN O USEN EL SERVICIO HOSPEDADO.

Licencias

LOS TÉRMINOS DE LICENCIA DE SOFTWARE DISPONIBLES EN EL SITIO WEB DE AVAYA, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, EN EL ENLACE “TÉRMINOS DE LICENCIA DE SOFTWARE DE AVAYA (Productos de Avaya)” O EN EL SITIO WEB POSTERIOR DESIGNADO POR AVAYA, SE APLICAN A CUALQUIER PERSONA QUE DESCARGUE, USE O INSTALE SOFTWARE DE AVAYA, ADQUIRIDO DE AVAYA INC., CUALQUIER SUBSIDIARIA DE AVAYA O UN CHANNEL PARTNER DE AVAYA (SEGÚN CORRESPONDA) BAJO UN ACUERDO COMERCIAL CON AVAYA O CON UN CHANNEL PARTNER DE AVAYA. A MENOS QUE AVAYA ACUERDE LO CONTRARIO POR ESCRITO, AVAYA NO OTORGA ESTA LICENCIA SI EL SOFTWARE FUE OBTENIDO DE ALGUIEN DISTINTO A AVAYA, UNA SUBSIDIARIA DE AVAYA O UN CHANNEL PARTNER DE AVAYA, RESERVÁNDOSE AVAYA EL DERECHO A EJERCER ACCIONES LEGALES EN SU CONTRA O EN CONTRA DE TERCEROS QUE USEN O VENDAN EL SOFTWARE SIN UNA LICENCIA. AL INSTALAR, DESCARGAR O UTILIZAR EL SOFTWARE, O AL AUTORIZAR A TERCEROS A HACERLO, USTED, EN NOMBRE DE SÍ MISMO Y DE LA ENTIDAD PARA LA QUE ESTÁ INSTALANDO, DESCARGANDO O UTILIZANDO EL SOFTWARE (EN ADELANTE, A LOS QUE SE HACE REFERENCIA INDISTINTAMENTE COMO “USTED” Y “USUARIO FINAL”), ACEPTAN ESTOS TÉRMINOS Y CONDICIONES, Y CREAN UN CONTRATO VINCULANTE ENTRE USTED Y AVAYA INC. O LA SUBSIDIARIA DE AVAYA QUE CORRESPONDA (“AVAYA”).

Avaya le otorga una licencia dentro del alcance de los tipos de licencia que se describen a continuación, con la excepción de Heritage Nortel Software, para el que se detalla el alcance de la licencia a continuación. Siempre que la documentación de la orden no identifique expresamente un tipo de licencia, la licencia aplicable será una Licencia de sistema designado según se establece a continuación en la sección de Licencia de sistema designado (DS), según corresponda. La cantidad correspondiente de licencias y unidades de capacidad para la que se otorga la licencia será uno (1), a menos que una cantidad diferente de licencias o unidades de capacidad se especifique en la documentación u otros materiales disponibles para usted. “Software” significa programas de computadora en código objeto proporcionado por Avaya o un Channel Partner de Avaya, ya sea como productos independientes o preinstalados en productos de hardware, y cualquier mejora, actualización, revisión, corrección de falla o versiones modificadas del mismo. “Procesador designado” significa un dispositivo informático independiente único. “Servidor” significa un conjunto de Procesadores designados que aloja (ya sea física o virtualmente) una aplicación de software a la que pueden acceder varios usuarios. “Instancia” significa una única copia del software que se ejecuta en un momento determinado: (i) en una máquina física, o (ii) en un software instalado en una máquina virtual (“VM”) o una implementación similar.

Tipos de licencia

Licencia de sistemas designados (DS). El usuario final puede instalar y utilizar cada copia o una instancia del software únicamente: 1) en una cantidad de procesadores designados hasta el número que indica la orden; o 2) hasta la cantidad de instancias del software que indica la orden, la documentación o según lo autorice Avaya por escrito. Avaya puede exigir que el procesador designado sea indicado en la orden por tipo, número de serie, tecla de función, instancia, ubicación u otra designación específica, o que el usuario final proporcione a Avaya a través de medios electrónicos establecidos por Avaya específicamente para este propósito.

Licencia de usuarios simultáneos (CU). El usuario final puede instalar y usar el Software en varios Procesadores designados o en uno o más Servidores, siempre y cuando sólo el número de Unidades con licencia obtenga acceso y use el Software en cualquier momento dado, según se indica en la orden, la

documentación o según lo autorice Avaya por escrito. Una “unidad” se refiere a la unidad en la que Avaya, a su exclusivo criterio, fundamenta el precio de sus licencias y puede ser incluso, entre otros, un agente, puerto o usuario, una cuenta de correo electrónico o de correo de voz en nombre de una persona o función corporativa (por ejemplo, administrador web o centro de asistencia técnica) o una entrada de directorio en la base de datos administrativa utilizada por el software que permite que un usuario se conecte con el software. Las unidades pueden vincularse con un servidor específico identificado o una instancia del software.

Licencia de clúster (CL). El usuario final puede instalar y usar cada copia o una instancia del software solo hasta alcanzar la cantidad de clústeres que se indica en la orden, la documentación, o según lo autorice Avaya por escrito con una cantidad predeterminada de un [1] clúster, si no se indica.

Licencia empresarial (EN). El usuario final puede instalar y utilizar cada copia de una instancia del software solo para el uso de toda la empresa de una cantidad ilimitada de instancias del software según se indica en la orden, la documentación o según lo autorice Avaya por escrito.

Licencia del usuario identificado (NU). El usuario final puede: (i) instalar y utilizar cada copia o instancia del software en un solo procesador designado o servidor por usuario identificado autorizado (se define a continuación); o (ii) instalar y utilizar cada copia o instancia del software en un servidor siempre y cuando únicamente los usuarios identificados autorizados obtengan acceso y utilicen el software según se indica en la orden, la documentación, o según lo autorice Avaya por escrito. “Usuario identificado” se refiere a un usuario o dispositivo que ha sido expresamente autorizado por Avaya para tener acceso al software y utilizarlo. A entera discreción de Avaya, un “usuario identificado” puede ser incluso, entre otros, designado por nombre, función corporativa (por ejemplo, administrador web o centro de asistencia técnica), una cuenta de correo electrónico o de correo de voz a nombre de una persona o función corporativa, o una entrada de directorio en la base de datos administrativa utilizada por el software que permite que un usuario se conecte con el software.

Licencia Shrinkwrap (SR). El usuario final puede instalar y utilizar el software de acuerdo con los términos y las condiciones de los contratos de licencia vigentes, como las licencias “shrinkwrap” o “clickthrough” que acompañan o se aplican al software (“licencia shrinkwrap”) según se indica en la orden, la documentación, o según lo autorice Avaya por escrito.

Licencia de transacción (TR). El usuario final puede utilizar el software hasta la cantidad de transacciones que se especifica durante el período de tiempo especificado y según se indica en la orden, la documentación, o según lo autorice Avaya por escrito. Una “Transacción” significa la unidad a partir de la cual Avaya, a su solo criterio, basa la fijación de precio de su licenciamiento y puede ser, sin limitación, medida por el uso, acceso, interacción (entre el cliente/servidor o cliente/organización), u operación del Software dentro de un período de tiempo especificado (por ejemplo, por hora, por día, por mes). Algunos ejemplos de transacciones incluyen, a mero título enunciativo, cada saludo reproducido / mensaje en espera habilitado, cada promoción personalizada (en cualquier canal), cada operación de devolución de llamada, cada agente en vivo o sesión de chat en web, cada llamada enrutada o redirigida (en cualquier canal). El usuario final no puede exceder la cantidad de Transacciones sin el consentimiento previo de Avaya y el pago de una tasa adicional.

Heritage Nortel Software

“Heritage Nortel Software” significa el software que adquirió Avaya como parte de la compra de Nortel Enterprise Solutions Business en diciembre de 2009. El Heritage Nortel Software es el software contenido en la lista de productos Heritage Nortel Products ubicada en https://support.avaya.com/LicenseInfo en el enlace “Heritage Nortel Products” o el sitio web posterior designado por Avaya. Para el software Nortel heredado, Avaya otorga al cliente una licencia para utilizar el software Nortel heredado en virtud del presente documento únicamente en la medida de la activación autorizada o el nivel de uso autorizado, únicamente para el propósito especificado en la documentación y solamente como se incorpora, ejecuta o para comunicación con equipo Avaya. Los cargos por Heritage Nortel Software se podrían basar en el alcance de activación o el uso autorizado según se especifique en una orden o factura.

Copyright

Excepto donde se indique expresamente lo contrario, no se debe hacer uso de los materiales de este sitio, de la documentación, del software, del servicio alojado ni del hardware proporcionados por Avaya. Todo el contenido de este sitio, la documentación, el servicio alojado y los productos proporcionados por Avaya, incluida la selección, la disposición y el diseño del contenido, son de propiedad de Avaya o de sus licenciantes y están protegidos por leyes de derecho de autor y otras leyes de propiedad intelectual, incluidos los derechos de su género relacionados con la protección de las bases de datos. No debe modificar, copiar, reproducir, reeditar, cargar, publicar, transmitir ni distribuir de ninguna manera el contenido, en su totalidad o en parte, incluidos los códigos y el software, a menos que posea una autorización expresa de Avaya. La reproducción, transmisión, difusión, almacenamiento y/o uso no autorizado sin el consentimiento expreso por escrito de Avaya puede considerarse un delito penal o civil según la ley vigente.

Virtualización

Si el producto se implementa en una máquina virtual, se aplica lo siguiente. Cada producto tiene su propio código de pedido y tipos de licencia. A menos que se indique lo contrario, cada instancia de un producto debe pedirse por separado y tener una licencia independiente. Por ejemplo, si el cliente usuario final o el Channel Partner de Avaya prefieren instalar dos instancias del mismo tipo de producto, entonces se deben solicitar dos productos del mismo tipo.

Componentes de terceros

“Componentes de terceros” se refieren a ciertos programas de software y partes de estos incluidos en dicho software o servicio alojado que pueden contener software (incluido el software de código abierto) distribuido según contratos de terceros (“Componentes de terceros”), que incluyen condiciones sobre los derechos a utilizar ciertas partes del software (“Términos y condiciones de terceros”). Según se requiera, la información con respecto al código fuente de SO Linux distribuido (para aquellos productos que tienen código fuente de SO Linux distribuido) y que identifique a los titulares de derechos de autor de componentes de terceros y los términos y las condiciones de terceros que se aplican está disponible en los productos, la documentación o en el sitio web de Avaya: https://support.avaya.com/Copyright o el sitio web posterior designado por Avaya. Los términos de la licencia de software de código abierto que se proporcionan como Términos de terceros se corresponden con los derechos de licencia otorgados en estos Términos de licencia de software y pueden contener derechos adicionales que lo beneficien, como la modificación y distribución del software de código abierto. Los Términos de terceros tienen prioridad sobre estos Términos de licencia de software, únicamente con respecto a los Componentes de terceros aplicables, en la medida en que estos Términos de la licencia de software impongan mayores restricciones que los Términos de terceros aplicables.

Lo siguiente corresponde solo si el códec H.264 (AVC) se distribuye con el producto. ESTE PRODUCTO ESTÁ SUJETO A LA LICENCIA DE CARTERA DE PATENTES AVC PARA EL USO PERSONAL DE UN CONSUMIDOR Y OTROS USOS QUE NO IMPLIQUEN REMUNERACIÓN PARA (i) CODIFICAR VÍDEO QUE CUMPLA CON EL ESTÁNDAR AVC (“AVC VIDEO”) O (ii) DECODIFICAR VÍDEO AVC QUE UN CLIENTE CODIFICÓ DURANTE UNA ACTIVIDAD PERSONAL U OBTENIDO A TRAVÉS DE UN PROVEEDOR DE VÍDEO AUTORIZADO PARA SUMINISTRAR VÍDEO AVC. NO SE OTORGA LICENCIA NI SE IMPLICA PARA CUALQUIER OTRO USO. PARA OBTENER INFORMACIÓN ADICIONAL, PUEDE CONSULTAR MPEG LA, L.L.C. VISITE HTTP://WWW.MPEGLA.COM.

Proveedor de servicio

LO SIGUIENTE SE APLICA A LOS CHANNEL PARTNERS DE AVAYA QUE ALOJEN PRODUCTOS O SERVICIOS DE AVAYA. EL PRODUCTO O SERVICIO ALOJADO PUEDE USAR COMPONENTES DE TERCEROS SUJETOS A LOS TÉRMINOS DE TERCEROS Y REQUERIR QUE EL PROVEEDOR DE SERVICIOS TENGA UNA LICENCIA INDEPENDIENTE DIRECTA DE ESTOS TERCEROS. UN CHANNEL PARTNER DE AVAYA QUE ALOJE PRODUCTOS DE AVAYA DEBE CONTAR CON AUTORIZACIÓN ESCRITA DE AVAYA, Y, EN CASO DE QUE DICHOS PRODUCTOS ALOJADOS UTILICEN O INCORPOREN SOFTWARE DE TERCEROS, LO QUE INCLUYE, A TÍTULO ENUNCIATIVO, SOFTWARE O CÓDECS DE MICROSOFT, EL CHANNEL PARTNER DE AVAYA DEBERÁ OBTENER DE FORMA INDEPENDIENTE Y A SU CARGO LOS ACUERDOS DE LICENCIA CORRESPONDIENTES, DIRECTAMENTE DEL PROVEEDOR DE TERCEROS.

CON RESPECTO A LOS CÓDECS, SI EL CHANNEL PARTNER DE AVAYA ALOJA PRODUCTOS QUE UTILIZAN O INCORPORAN LOS CÓDECS H.264 O H.265, EL CHANNEL PARTNER DE AVAYA RECONOCE Y MANIFIESTA ESTAR DE ACUERDO CON QUE ES RESPONSABLE DE ASUMIR TODAS LAS TARIFAS Y/O REGALÍAS. EL CÓDEC H.264 (AVC) ESTÁ SUJETO A LA LICENCIA DE CARTERA DE PATENTES AVC PARA EL USO PERSONAL DE UN CONSUMIDOR Y OTROS USOS QUE NO IMPLIQUEN REMUNERACIÓN PARA (I) CODIFICAR VÍDEO QUE CUMPLA CON EL ESTÁNDAR AVC (“AVC VIDEO”) O (II) DECODIFICAR VÍDEO AVC QUE UN CONSUMIDOR CODIFICÓ DURANTE UNA ACTIVIDAD PERSONAL U OBTENIDO A TRAVÉS DE UN PROVEEDOR DE VÍDEO AUTORIZADO PARA SUMINISTRAR VÍDEO AVC. NO SE OTORGA LICENCIA NI SE IMPLICA PARA CUALQUIER OTRO USO. INFORMACIÓN ADICIONAL SOBRE LOS CÓDECS H.264 (AVC) y H.265 (HEVC) PUEDE SER OBTENIDA DE MPEG LA, L.L.C. VISITE HTTP://WWW.MPEGLA.COM.

Cumplimiento de leyes

Usted reconoce y acepta que es su responsabilidad respetar las leyes y los reglamentos aplicables, incluidos, a mero título enunciativo, las leyes y los reglamentos relacionados con la grabación de llamadas, la privacidad de datos, la propiedad intelectual, el secreto comercial, el fraude, los derechos de interpretación musical, en el país o territorio en el cual se utiliza el producto de Avaya.

Prevención del fraude telefónico

El “fraude telefónico” se refiere al uso no autorizado de su sistema de telecomunicaciones por parte de un participante sin autorización (por ejemplo, una persona que no es un empleado, agente ni subcontratista corporativo o una persona que no trabaja en nombre de su compañía). Tenga en cuenta que pueden existir riesgos de fraude telefónico asociados con su sistema y que, en tal caso, esto puede generar cargos adicionales considerables para sus servicios de telecomunicaciones.

Intervención en fraude telefónico de Avaya

Si sospecha que es víctima de fraude telefónico y necesita asistencia o soporte técnico, llame a la línea directa de Intervención en Fraude Telefónico del Centro de Servicio Técnico al +1-800-643-2353 para Estados Unidos y Canadá. Para obtener números de teléfono de soporte técnico adicionales, visite el sitio web de Soporte Técnico de Avaya: https://support.avaya.com o el sitio web posterior designado por Avaya.

Vulnerabilidades de seguridad

Puede encontrar información sobre las políticas de respaldo de seguridad de Avaya en la sección de Soporte Técnico y políticas de seguridad de https://support.avaya.com/security.

Las sospechas de vulnerabilidades de la seguridad de productos de Avaya se manejan a través del Flujo de soporte técnico de seguridad de productos de Avaya (https://support.avaya.com/css/P8/documents/100161515).

Marcas comerciales

Las marcas comerciales, logotipos y marcas de servicio (“Marcas”) que aparecen en este sitio, la documentación, los servicios alojados y los productos proporcionados por Avaya son marcas registradas o no registradas de Avaya, sus afiliados, licenciantes, proveedores y otros terceros. Los usuarios no tienen permiso de usar dichas Marcas sin previo consentimiento por escrito de Avaya o dichos terceros que puedan ser propietarios de la Marca. Ningún contenido de este sitio, la documentación, los servicios alojados ni los productos deben considerarse como otorgamiento, por implicación, impedimento o de alguna otra forma, una licencia o derecho para usar las Marcas sin la autorización expresa por escrito de Avaya o del tercero correspondiente.

Avaya es una marca registrada de Avaya Inc.

Todas las demás marcas son propiedad de sus respectivos dueños.

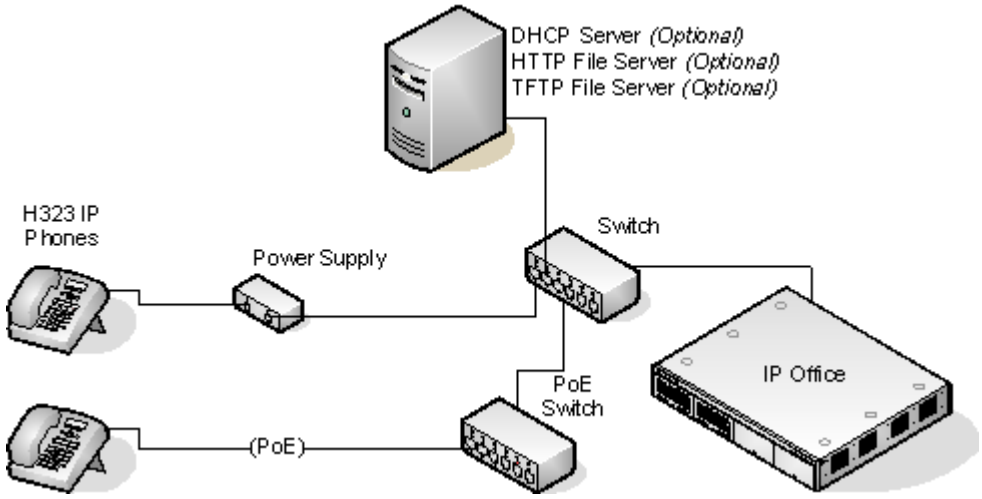
Linux® es una marca comercial registrada de Linus Torvalds en EE. UU. y en otros países.

Contenido

Parte 1: Instalación del teléfono IP Office H323

Capítulo 1: Teléfonos IP Office H.323

Esta documentación proporciona notas acerca de la instalación de teléfonos IP de Avaya compatibles en un sistema IP Office. Debe utilizarse junto con la documentación de instalación existente para los teléfonos de esas series.



- **Instalación de DHCP frente a IP fija:** si bien la instalación de direcciones IP fijas de los teléfonos IP H.323 es posible, se recomienda fehacientemente realizar la instalación mediante DHCP. El uso de DHCP facilita el proceso de instalación y el mantenimiento y la administración en el futuro. Para las instalaciones fijas, después de una actualización del archivo de inicio, todos los valores de configuración de la dirección fija se perderán y deberán volver a ingresarse.
- **Evaluación de red:** la transmisión de voz de alta calidad en la red IP requiere una evaluación minuciosa de una gran cantidad de factores. Por lo tanto:
  - Recomendamos vehementemente que la instalación del teléfono IP sólo sea realizada por instaladores con experiencia en VoIP.
  - Toda la red del cliente debe ser evaluada antes de la instalación para saber si es apropiada para VoIP. Avaya no brindará asistencia técnica en cualquier instalación donde los resultados de la evaluación de una red no puedan suministrarse. Consulte Evaluación de red en la página 18 para obtener más detalles.

Vínculos relacionados

Novedades de esta versión en la página 11
Teléfonos IP H.323 compatibles en la página 11
Capacidad del sistema en la página 12
Firmware de teléfonos en la página 13
Generación automática de archivos en la página 14
Instalación simple en la página 14

Novedades de esta versión

Este manual incluye los siguientes cambios introducidos en la versión 11.1 de IP Office:

- Funcionamiento del modo de suscripción: los sistemas IP Office ahora pueden ejecutarse en modo de suscripción. En ese modo, la autorización para los teléfonos IP para operar con el sistema se otorga mediante asociación con un usuario suscrito en lugar de una licencia de extensión. El modo de suscripción solo es compatible con los siguientes teléfonos Avaya H323:
  - Serie 1600: 1603IP/SW, 1608, 1608-I, 1616, 1616-I.
  - Serie 3600: 3641, 3645.
  - Serie 3700: 3720, 3725, 3730, 3735, 3740, 3745, 3749 - Conexión por medio de estaciones base DECT R4.
  - Serie 9600: 9608, 9608G, 9611G, 9621G, 9641G, 9641GS.

Vínculos relacionados

Teléfonos IP Office H.323 en la página 10

Teléfonos IP H.323 compatibles

Esta documentación contiene notas de instalación para los teléfonos Avaya que se detallan a continuación. Otros teléfonos IP H.323 de Avaya compatibles, como por ejemplo los de la serie DECT R4 3700, están cubiertos por documentación de instalación diferente.

Teléfonos IP H.323		PoE Clase		Puerto PC	Modo de suscripción
		Clase	Desocupado		
Serie 1600	1603	2	4,4W	-	✓
	1603SW	2	4,4W	✓	✓
	1608	2	3,7W	✓	✓
	1616	2	2,7W	✓	✓
Serie 9600	9608	1	2,08W	✓	✓
	9611G	1	2,8W	✓	✓
	9621G	2	3,49W	✓	✓
	9641G	2	3,44W	✓	✓

- 1603/1603SW - Estos teléfonos requieren un divisor PoE para poder utilizar PoE.

Vínculos relacionados

Teléfonos IP Office H.323 en la página 10

Capacidad del sistema

La capacidad del sistema abarca la cantidad de extensiones configurables del teléfono y el número de llamadas simultáneas del teléfono IP.

Capacidad de extensión

La cantidad máxima de teléfonos IP H.323 IP compatibles depende del tipo de sistema.

Los sistemas IP500 V2 admiten hasta 384 extensiones. Para conocer la capacidad de los teléfonos IP, reste la cantidad de puertos de extensiones físicas no IP instaladas en el sistema, es decir, los puertos de extensión de la unidad de control de IP Office y cualquier módulo de expansión externo. No obstante, tenga en cuenta que estos sistemas solo admiten 148 canales VCM como máximo, lo que puede restringir la cantidad de llamadas VoIP simultáneas. Consulte a continuación.

En el caso de sistemas IP Office Server Edition, la capacidad de la extensión IP depende del tipo de servidor. Consulte el documento Avaya Pautas de IP Office™ Plataform: capacidad.

Capacidad de llamadas

Existen determinadas situaciones en las que el sistema IP500 V2 debe proporcionar un canal de compresión de voz para que un teléfono IP pueda realizar llamadas. Estos canales son proporcionados por los Módulos de compresión de voz (VCM) instalados en el sistema. La cantidad de canales VCM necesarios y el tiempo durante el que se necesitan depende de varios factores.

A continuación figura un resume simple:

- Durante el establecimiento de llamadas se requiere un canal VCM.
- El canal VCM se libera si la llamada se realiza o se recibe a través de otro dispositivo IP mediante el mismo códec de compresión (los códecs VC; compatibles son G.711, G.729 y G.722).
- El canal VCM se utiliza para la duración de la llamada cuando ésta se realiza o se recibe a través de un dispositivo no IP (extensión o línea troncal).

- Se debe recordar que los canales VCM también se utilizan para llamadas realizadas desde dispositivos no IP a líneas IP si estos se configuran en el sistema IP Office (líneas IP, SIP y SES).
- Las llamadas realizadas desde dispositivos no IP al servidor de correo de voz de IP Office utilizan un canal VCM.

Vínculos relacionados

Teléfonos IP Office H.323 en la página 10

Firmware de teléfonos

El firmware que usan los teléfonos IP de Avaya puede actualizarse y pueden adquirirse diferentes versiones de firmware a través del sitio Web de asistencia técnica de Avaya. Sin embargo, los teléfonos IP H.323 que se usan en un sistema IP Office solo deben usar el firmware suministrado que viene preinstalado en el sistema IP Office o con su aplicación de IP Office Manager. Puede que otras versiones del firmware del teléfono IP no se hayan probado específicamente con los sistemas IP Office y no deben usarse a menos que se mencione específicamente la compatibilidad de IP Office en la documentación que viene con el firmware.

El firmware consta de varios tipos de archivos diferentes:

Tipo de archivo	Descripción
Archivos `xxupgrade`	El primer archivo que solicita un teléfono cuando se inicia es el archivo `xxupgrade`. Este archivo contiene una lista de los archivos .bin del teléfono que se encuentran disponibles como parte del conjunto de firmware y los números de versión de dichos archivos. Si la versión de un archivo es diferente a la que el teléfono ya cargó, el teléfono solicitará el nuevo archivo. Durante el proceso, el teléfono puede reiniciarse después de cargar cada uno de los archivos y luego, de ser necesario, puede volver a solicitar el archivo xxupgrade.txt hasta se haya actualizado todo su firmware. Se proporcionan archivos separados para las diferentes series de teléfonos. Por ejemplo: • `16xxupgrade.txt`: este archivo enumera los archivos de firmware que deben cargar los teléfonos de la serie 1600. • `96xxupgrade.txt`: este archivo enumera los archivos de firmware que deben cargar los teléfonos de la serie 9600. • `96x1Hupgrade.txt`: este archivo enumera los archivos de firmware que deben cargar los teléfonos de las series 9608, 9611, 9621 y 9641.
Archivos `.bin`	Siguiendo las instrucciones en el archivo `xxupgrade.txt`, el teléfono cargará los archivos .bin que se requieran en caso de que sus versiones sean diferentes de las que el teléfono ya ha cargado.
Archivos `.tar`	En lugar del archivo `.bin` que usan otros teléfonos, los teléfonos de la serie 9600 usan archivos .tar para descargar varios archivos en un solo paso y luego descomprimir los archivos .tar para cargar sus contenidos.

La tabla continúa…

Tipo de archivo	Descripción
Archivos `46xxsettings.txt`	La última línea del archivo `xxupgrade.txt` ordena al teléfono cargar un archivo `46xxsettings.txt`. Este es un archivo editable que puede usarse para ajustar el funcionamiento de los teléfonos.
Archivos `.lng`	El firmware puede incluir archivos de idioma para que usen los teléfonos de las serie 1600 y 9600. En el archivo `46xxsettings.txt` se establece cuáles de estos archivos de idiomas se cargan.

Los archivos de firmware del teléfono se instalan como parte de la aplicación IP Office Manager y se encuentran en el directorio de instalación de la aplicación. De manera predeterminada, el directorio se encuentra en `c:\Program Files\Avaya\IP Office\Manager`.

También pueden obtenerse directamente los mismos archivos de firmware desde el paquete de software que se utiliza para instalar IP Office Manager sin tener que llevar a cabo la instalación. Los archivos se encuentran en la subcarpeta `\program files\Avaya\IPOffice\Manager` del directorio de instalación.

Tenga en cuenta que estos conjuntos de archivos incluyen los archivos .bin que también se emplean para otros dispositivos, incluido el sistemaIP Office mismo.

Vínculos relacionados

Teléfonos IP Office H.323 en la página 10

Generación automática de archivos

Cuando el sistema IP Office está actuando como el servidor de archivos para los teléfonos, puede generar automáticamente los archivos `46xxsettings.txt` e .lng que usan los teléfonos. Hará esto si el archivo solicitado no está presente físicamente en la ubicación donde el sistema almacena los archivos de firmware. El sistema también utiliza los ajustes de configuración del usuario para generar automáticamente el archivo de configuración del usuario del teléfono.

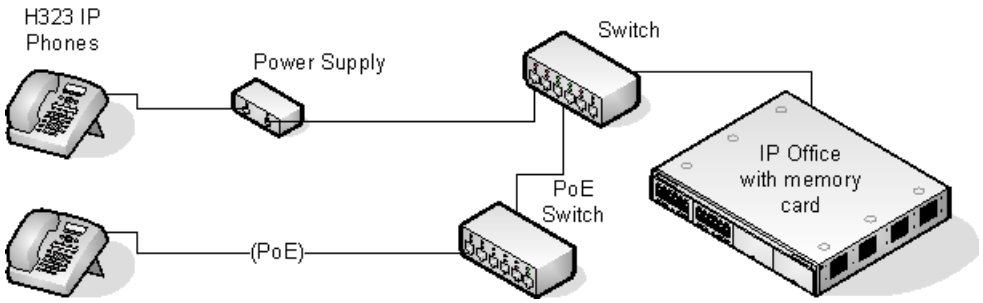
El sistema aún puede generar automáticamente archivos, incluso cuando se usa la redirección HTTP para cargar los archivos `.bin` de 9608, 9611, 9621 y 9641 desde otro servidor de archivos.

Vínculos relacionados

Teléfonos IP Office H.323 en la página 10

Instalación simple

La instalación más sencilla tiene el sistema IP Office que actúa como los servidores DHCP y de archivos para todos los teléfonos IP registrados en él.



Este tipo de instalación utiliza los siguientes equipos:

- **Servidor IP Office:** el sistema IP Office realiza varias funciones para los teléfonos:
  - **Servidor DHCP:** el sistema IP Office está actuando como el servidor DHCP para los teléfonos. La respuesta de DHCP a los teléfonos incluye configuración de dirección IP, detalles del servidor de archivos que se usa en la configuración de IP Office y los sistemas en la dirección como el gatekeeper de H.323 para los teléfonos. Es posible configurar la función DHCP de IP Office para que proporcione direcciones DHCP solo en respuesta a solicitudes de teléfonos IP de Avaya. Esto permite utilizar un servidor DHCP alternativo para otros dispositivos que utilicen DHCP.
  - **Gatekeeper de H.323:** los teléfonos IP requieren un gatekeeper de H.323 en el que deben registrarse. Luego, el gatekeeper controla la conexión de llamadas hacia y desde el teléfono. En este y todos los escenarios, los sistemas IP Office como el Gatekeeper de H.323.
  - **Servidor de archivos:** durante la instalación, los teléfonos IP deben descargar archivos de firmware para un servidor de archivos. Esto se hace usando HTTPS, HTTP o TFTP en ese orden (los teléfonos de la serie 1600 y 9600 no son compatibles con TFTP). La tarjeta de memoria de la unidad de control de IP Office puede usarse como fuente de archivo.
  - Los sistemas IP500 V2 pueden actuar como servidor de archivos para hasta 50 teléfonos usando su propia tarjeta de memoria. Los sistemas IP Office Server Edition también pueden actuar como servidor de archivos para hasta 50 teléfonos. Para mayores cantidades, debe usarse un servidor HTTP de terceros aparte.
  - **Servidor de copia de seguridad/restauración:** los teléfonos de la serie 1600 y 9600 pueden configurarse para que hagan copia de seguridad y restauración en un servidor de la configuración del usuario y del teléfono. La dirección de este servidor se configura por separado de la del servidor de archivos que se utiliza para firmware del teléfono a través del mismo servidor que se puede usar. El método recomendado es emplear el sistema IP Office como el servidor para esta función.
- **Conmutadores:** el IP Office tiene una cantidad limitada de puertos de conexión LAN, que tienen por objeto solo conectarse a la red de datos existente. Para agregar teléfonos IP es necesario que la red incluya capacidad de puerto adicional.
- **Fuentes de alimentación:** cada teléfono IP H.323 necesita una fuente de alimentación. El sistema IP Office no proporciona alimentación a los teléfonos IP. Los teléfonos pueden ser:
  - **Fuente de alimentación a través de Ethernet:** la mayoría de los teléfonos IP de Avaya pueden alimentarse por medio de una fuente de alimentación a través de Ethernet (PoE) 802.3af. Esto puede hacerse usando conmutadores PoE para que

admitan varios teléfonos o mediante el uso de dispositivos inyectores PoE individuales para cada teléfono.

- **Unidades de fuente de alimentación individual:** con cada teléfono puede utilizarse una fuente de alimentación individual. Para ello, se deberá contar con una toma de energía eléctrica en la ubicación de cada teléfono. El tipo de fuente de alimentación dependerá del tipo de teléfono. Tenga en cuenta que es posible que los teléfonos que usan módulos de botones necesiten usar una unidad de alimentación individual en lugar de PoE.

Vínculos relacionados

Teléfonos IP Office H.323 en la página 10

Requerimientos de instalación

Para instalar un teléfono IP en IP Office, se requieren los siguientes elementos:

	Descripción
Evaluación de red	Debe realizarse una evaluación de red. Avaya no admitirá VoIP en una red donde no se haya obtenido una evaluación de red satisfactoria.
Información del número de extensión y el usuario	Se necesita una lista completa de la información del número de extensión planificado y el nombre de usuario. El número de extensión planificado no debe estar en uso y el teléfono lo solicitará durante la instalación.
Suministros de energía	Los teléfonos requieren una fuente de suministro de energía. Los teléfonos IP de Avaya no utilizan energía de la unidad de IP Office. Existen varias opciones para la manera en que suministra la fuente de alimentación a los teléfonos y todos los teléfonos de escritorio IP de Avaya admiten fuente de alimentación a través de Ethernet (PoE). Consulte Opciones de fuentes de alimentación en la página 23
Toma LAN	Se requiere un punto de conexión LAN Ethernet RJ45 para cada teléfono.
Cableado categoría 5	Todos los cables LAN y la infraestructura de cables LAN que se utilicen con los teléfonos IP H.323 deben usar cableado CAT5.
Cables LAN	Verifique que se haya suministrado un cable LAN RJ45 con el teléfono IP para realizar la conexión con la fuente de alimentación. También puede contar con un cable LAN RJ45 para realizar la conexión desde la fuente de alimentación hasta la red LAN del cliente. Esto dependerá del tipo de fuente de alimentación que se va a usar. Puede utilizarse otro cable LAN RJ45 para conectar la PC del usuario a la red LAN a través del teléfono IP (no compatible con los teléfonos IP H.323 4601, 4602, 5601 y 5602).
Canales de compresión de voz	En el caso de los sistemas IP500 V2, la unidad de control debe tener canales de compresión de voz instalados. Los canales son necesarios durante la conexión si las llamadas involucran teléfonos IP y es posible que también se necesiten durante la llamada. Consulte Canales de compresión de voz en la página 19 para obtener todos los detalles.

La tabla continúa…

	Descripción
Servidor de DHCP	La unidad de IP Office puede realizar esta función para todos los teléfonos. Si se usa otro servidor DHCP para la red, es posible que DHCP se utilice para los teléfonos IP H.323; consulte Servidores DHCP alternativos. Igualmente, el sistema IP Office puede configurarse para que solo proporcione compatibilidad con DHCP para teléfonos IP de Avaya. • Las direcciones IP fijas también pueden emplearse para instalación de teléfonos IP si es necesario. Sin embargo, no se recomienda ese método de instalación.
Servidor de archivos HTTP	Una PC que ejecuta la aplicación IP Office Manager puede realizar esta función para hasta cinco (5) teléfonos IP H.323. Una unidad de control de IP Office con una tarjeta de memoria puede utilizar esa tarjeta como la fuente de hasta 50 teléfonos. El sistema IP Office puede actuar como el servidor de archivos para hasta 50 teléfonos IP. Para mayores cantidades, debe usarse un servidor HTTP de terceros aparte.
Gatekeeper de H.323	El sistema IP Office lleva a cabo esta función.
PC que ejecuta la aplicación Manager	Se requiere una PC con Windows que ejecuta IP Office Manager para cambiar la configuración de IP Office. La PC también debe tener System Status Application y System Monitor instalados.
Software de teléfono IP	El software para la instalación del teléfono IP se instala en la carpeta del programa de la aplicación IP Office Manager durante la instalación de aplicaciones. También se incluye como parte de la instalación de aplicaciones IP Office Server Edition de la aplicación IP Office en el servidor.
Licencias y suscripciones	Para sistemas que no se ejecutan en modo de suscripción, cada teléfono IP registrado con el sistema requiere una licencia para funcionar. En sistemas en modo de suscripción, la extensión debe estar asociada con un usuarios suscrito. Consulte Licencias y suscripciones.
Servidor de copia de seguridad/restauración	Los teléfonos hacen copias de seguridad y restauran diversas configuraciones de teléfonos y usuarios cuando el usuario inicia y cierra sesiones. Para esto se usan los archivos almacenados en un servidor de archivos. Este no es necesariamente el mismo servidor que se utiliza para los archivos de firmware del teléfono. Para esta función es posible usar el almacenamiento de archivos propio del sistema IP Office y es la opción recomendada.

Vínculos relacionados

Teléfonos IP Office H.323 en la página 10

Licencias y suscripciones

Suscripciones

Los sistemas que se ejecutan en modo de suscripción admiten extensiones hasta la cantidad total de suscripciones de usuario disponibles.

Licencias

Para sistemas que no se ejecutan en modo de suscripción, se requieren licencias para cada extensión IP.

- En sistemas IP Office Server Edition, el usuario debe estar configurado con un perfil de usuario con licencia, como una licencia de Usuario básico. Los usuarios sin licencia no pueden iniciar sesión en una extensión.
- Para teléfonos Avaya, se requiere una licencia Avaya IP Endpoint para cada teléfono. Esto incluye todos los teléfonos 1600, 9600, IP DECT, DECT R4 y Spectralink.
- Para teléfonos IP que no son de Avaya, se requiere una licencia para terminal IP de terceros.
  - De forma predeterminada, cada teléfono IP de Avaya que se registra en el sistema IP Office utiliza una licencia, siguiendo el orden en que se registran. La licencia queda liberada cuando el teléfono registra su salida. No obstante, es posible reservar una licencia para determinados teléfonos y así garantizar que esos teléfonos siempre obtengan una. Esto se realiza a través de la configuración **Reservar licencia de terminal IP de Avaya** de cada extensión IP. En sistemas que utilizan concesión de licencias WebLM, esta opción está fija para reservar una licencia.
  - Los teléfonos Avaya IP sin una licencia aún pueden registrarse pero están limitados a realizar únicamente llamadas de emergencia (llamadas de código corto Marcar emergencia). El usuario vinculado se considera desconectado, y el teléfono muestra el mensaje "No license available" (Sin licencia disponible). Si hay disponible una licencia, se asigna a cualquier auricular DECT sin licencia primero y luego a cualquier otro teléfono Avaya sin licencia en el orden en el que los teléfonos se hayan registrado.

Vínculos relacionados

Teléfonos IP Office H.323 en la página 10
Reserva de licencias en la página 37

Evaluación de red

El sistema IP Office es un sistema de voz sobre IP (VoIP) puro. Todas las troncales y extensiones telefónicas se conectan al sistema mediante la red de datos de los clientes. Por lo tanto, es fundamental que se obtenga acceso a la red del cliente y que vuelva a ser configurada si es necesario para satisfacer las necesidades de tráfico VoIP.

Advertencia:

Al instalar teléfonos IP en un sistema IP Office, Avaya supone que se ha realizado una evaluación de red. Si se informa un problema de asistencia técnica a Avaya, Avaya puede solicitar acceso a los resultados de una evaluación de red reciente, y es posible que se niegue a brindar asistencia técnica si no se realizó una evaluación de red apropiada.

La tecnología actual permite que redes configuradas de forma óptima brinden servicios VoIP con calidad de voz similar a la de la red telefónica pública. Sin embargo, pocas redes se configuran de forma óptima, y por lo tanto se debe tener cuidado al evaluar la calidad de VoIP que puede alcanzarse en la red de un cliente.

No todas las redes pueden realizar transmisiones de voz. Algunas redes de datos no tienen capacidad suficiente para el tráfico de voz, o tienen picos de datos que, en ocasiones, afectarán el tráfico de voz. Además, el historial habitual de crecimiento y desarrollo de una red

al integrar productos de varios proveedores hace que sea necesario probar todos los componentes de la red para detectar la compatibilidad con el tráfico de VoIP.

Una evaluación de red debe incluir lo siguiente:

- Una auditoría de red para verificar el equipo existente y evaluar sus capacidades, incluida su capacidad de cubrir las necesidades actuales y previstas para voz y datos.
- Una determinación de los objetivos de la red, incluidos el tipo de tráfico predominante, la elección de tecnologías y el establecimiento de objetivos de calidad de voz.
- La evaluación debe dejar la certeza de que la red tendrá la capacidad para datos y tráfico de voz imprevistos.

Objetivos de la evaluación de red

Los objetivos de la evaluación de red son:

- Latencia: Menos de 180 ms para obtener una buena calidad. Menos de 80 ms para obtener una calidad de larga distancia. Esta es la medida del tiempo de transferencia de paquete en una dirección. Por lo general, es aceptable un rango de entre 80 ms y 180 ms. Es importante señalar que los diferentes nombres de audio utilizados imponen una demora fija causada por la conversión de nombres como se detalla a continuación:
  - G.711: 20ms.
  - G.722: 40ms.
  - G.729: 40ms.
- Pérdida de paquete: Menos del 3 % para obtener una buena calidad. Menos de 1 % para obtener una calidad de larga distancia. En caso de pérdida excesiva de paquetes, la comunicación se escuchará entrecortada y podrán producirse demoras para establecer la llamada.
- Fluctuación: Inferior a 20 ms. La vibración es una medida de la discrepancia en el tiempo que tardan en llegar a su destino diferentes paquetes de la misma llamada. En caso de exceso de vibración, se escuchará un eco.
- Duración: Monitoree las estadísticas una vez por minuto durante una semana entera. La evaluación de red debe incluir las horas de actividad comercial habituales.

Vínculos relacionados

Teléfonos IP Office H.323 en la página 10

Canales de compresión de voz

Las llamadas hacia y desde dispositivos IP pueden requerir la conversión al formato de códec de audio utilizado por el dispositivo IP. En los sistemas IP Office, esta conversión se realiza mediante canales de compresión de voz. Estos son compatibles con los códecs de audio IP comunes G.711, G.722 y G.729a.

- En el caso de las unidades de control IP500 V2, pueden agregarse canales usando tarjetas VCM IP500 y tarjetas de combinación IP500.
- Los sistemas IP Office Server Edition proporcionan sus propios canales de compresión de voz a través del software sin requerir ningún hardware adicional.

Los canales de compresión de voz se usan de la siguiente manera.

Tipo de llamada	Uso de los canales de compresión de voz
Dispositivo IP a dispositivo no IP	Estas llamadas requieren de un canal de compresión de voz durante la duración de la llamada. Si no hay un canal disponible, la llamada recibe una indicación de ocupado.
Dispositivo IP a dispositivo IP	Los tonos de progreso de llamada (por ejemplo el tono de marcar, tono de marcar secundario, etc) no requieren canales de compresión de voz, con las siguientes excepciones: • La confirmación de código corto, campo ARS activado y tonos de entrada de código de cuenta requieren de un canal de compresión de voz. Cuando se conecta una llamada: • Si los dispositivos IP utilizan el mismo códec de audio, no se utiliza el canal de compresión de voz. Si los dispositivos utilizan distintos mismo códecs de audio, se requiere un canal de compresión de voz para cada uno.
Dispositivo no IP a dispositivo no IP	No se requieren canales de compresión de voz.
Música de espera	Proviene del bus TDM de IP Office y por tanto requiere un canal de compresión de voz cuando se reproduce en un dispositivo IP.
Recursos para conferencia y dispositivos IP	Los recursos de conferencia se administran desde el chip de conferencia, el cual se encuentra en el bus TDM de IP Office. Por tanto, se requiere un canal de compresión de voz para cada dispositivo IP incluidos en la conferencia. Esto incluye servicios que emplean recursos de conferencia como escucha, inctrusión de llamadas, grabación y monitoreo silencioso.
Dispositivos de servicios de correo de voz y dispositivos IP	Las llamadas a los servidores de correo de voz de IP Office son manejadas como llamadas de datos desde el bus TDM. Por tanto, todas las llamadas de un dispositivo IP a correo de voz requieren un canal decompresión de voz.
Llamadas de fax	Estas son llamadas de voz con un rango de frecuencia ligeramente más amplio que las llamadas de voz. IP Office soporta solamente las comunicaciones de fax por IP entre sistemas IP Office con la opción Transportar fax seleccionada. No es compatible actualimente con T38.
Llamadas de fax T38	IP Office 5.0 y posteriores es compatible con fax T38 en troncales SIP y extensiones SIP. Cada llamada de fax T38 emplea un canal VCM. Dentro de una Small Community Network, una llamada de fax T38 puede convertirse en una llamada a través de una línea SCN H.323 mediante el protocolo Soporte de transporte fax de IP Office. Esta conversión emplea dos canales VCM. A fin de usar una conexión de fax T38, puede establecerse la **Clasificación de equipo** de una extensión analógica conectada a una máquina de fax puede definirse como **Fax**. Además, está disponible una nueva función de código corto llamada **Marcar Fax**.

Nota:

Los dispositivos T3 IP deben configurarse en el tamaño de paquete de 20 ms para que puedan aplicar las condiciones anteriores. Si no se modifica la configuración de tamaño de paquete de 10 ms, se requerirá un canal de compresión de voz para todos los tonos y para las llamadas desde medios no directos.

Medición del uso de los canales

IP Office System Status Application permite visualizar el uso del canal de compresión de voz. En la sección Recursos aparece el número del canal en uso. También muestra la frecuencia con la que han ocurrido insuficientes canales disponibles, y la última vez que ocurrió este evento.

En el caso de las tarjetas VCM IP500, las luces LED (de 1 a 8) ubicadas en la parte delantera de la tarjeta VCM IP500 también indican el nivel de uso del canal.

Vínculos relacionados

Teléfonos IP Office H.323 en la página 10

CdS

Al transportar voz a través de enlaces de baja velocidad es posible que los paquetes de datos normales (paquetes de 1500 bytes) demoren o impidan que los paquetes de voz (por lo general 67 ó 31 bytes) atraviesen el enlace. Esto puede dar lugar a una calidad de voz inaceptable.

Por lo tanto, es de importancia fundamental que todos los conmutadores y enrutadores de tráfico de la red tengan alguna forma de mecanismo de calidad de servicio (QoS). Los enrutadores de QoS son esenciales para garantizar una latencia de voz baja y para mantener una calidad de audio suficiente.

IP Office admite el mecanismo DiffServ (RFC2474) QoS. Esto se basa en el uso de un campo Type of Service (ToS) (Tipo de servicio) en el encabezado del paquete IP. En sus interfaces WAN, IP Office utiliza esto para priorizar los paquetes de voz y señalización de voz. También fragmenta grandes paquetes de datos y, donde se admita, ofrece compresión de encabezado VoIP para minimizar la sobrecarga WAN.

Vínculos relacionados

Teléfonos IP Office H.323 en la página 10

Problemas potenciales de VoIP

Es probable que la presencia de una falla en una red, independientemente de su causa, inicialmente se manifieste como una degradación en la calidad de funcionamiento de VoIP. Esto es independientemente de si la falla está relacionada con el equipo de telefonía VoIP. Por lo tanto, al instalar una solución VoIP, debe tener conciencia de que se convertirá en el primer punto de contacto para diagnosticar y evaluar todos los problemas potenciales de la red del cliente.

	Descripción
Estándares de extremo a extremo coincidentes	VoIP depende de la compatibilidad y la selección de los mismos estándares de compresión de voz, compresión de encabezado y calidad de servicio (QoS) en todas las etapas del enrutamiento de llamadas. Los puntos de inicio y finalización deben utilizar los mismos métodos de compresión. Todos los puntos intermedios deben ser compatibles con DiffServ QoS.
Evitar hubs	Los hubs introducen eco y puntos de congestión. Si la red del cliente requiere conexiones LAN más allá de la capacidad de la unidad de IP Office, deberán utilizarse conmutadores Ethernet. Incluso si este no es el caso, se recomiendan conmutadores Ethernet, ya que permiten que se implemente la priorización de tráfico para dispositivos VoIP.
Acondicionamiento de la fuente de alimentación, protección y respaldo	Los sistemas telefónicos tradicionales suministran energía eléctrica a todos los dispositivos telefónicos conectados desde una sola fuente. En una instalación de VoIP, el mismo cuidado y la misma preocupación que se tiene al proporcionar acondicionamiento de la fuente de alimentación, protección y respaldo al sistema telefónico central debe aplicarse a todos los dispositivos de la red IP.
Multidifusión	En una red de datos, es posible que una tarjeta hub o una impresora que se instaló de forma incorrecta realice una multidifusión de tráfico sin que la falla se identifique de inmediato. En una red VoIP la multidifusión incorrecta afectará rápidamente las funciones y llamadas VoIP.
Direcciones IP duplicadas	Las direcciones duplicadas son un problema frecuente.
Uso excesivo	Un puesto de trabajo que transmite constantemente altos niveles de tráfico puede saturar una red, lo que puede generar la desaparición del servicio VoIP.
Acceso a la red	Una red IP es mucho más abierta a los usuarios que conectan un nuevo dispositivo o instalan software en dispositivos existentes y que luego tiene un impacto en VoIP.
Conexiones de cableado	Técnicamente, VoIP puede (siempre que el ancho de banda lo permita) ejecutarse en cualquier conexión de red IP. En la práctica, el cableado Cat5 es esencial.

Vínculos relacionados

[Teléfonos IP Office H.323](#) en la página 10

Conexión de la PC del usuario

Para simplificar la cantidad de conexiones LAN desde el escritorio del usuario, es posible enrutar el cable LAN Ethernet de la PC mediante la mayoría de los teléfonos IP de Avaya.

El cable LAN debe conectarse desde la PC hasta la toma que tenga un símbolo de PC (🖳) ubicado en la parte posterior del teléfono IP. La configuración de la red de la PC que se utilizó anteriormente para establecer una conexión directa con la red LAN no debe modificarse. Este puerto admite conexiones Ethernet 10/100 Mbps. Los teléfonos con un sufijo G también admiten conexiones Gigabit de 1000Mbps.

Para teléfonos sin un puerto para PC, debe utilizarse un adaptador Gigabit independiente (SAP 700416985). Este dispositivo divide el tráfico de datos y voz antes de que llegue al

teléfono, y proporciona una salida de 10/100Mbps para el teléfono y una salida de 10/100/1000Mbps para la PC. El adaptador recibe corriente de la fuente de alimentación existente del teléfono. Consulte "*Instalación del adaptador Gigabit Ethernet e instrucciones de seguridad*" (16-601543).

Vínculos relacionados

Teléfonos IP Office H.323 en la página 10

Opciones de fuentes de alimentación

Cada teléfono IP H.323 necesita una fuente de alimentación. No utilizan energía del sistema telefónico. A continuación figura una lista de opciones de fuentes de alimentación que pueden utilizarse.

IEEE 802.3af es un estándar que habitualmente se conoce como fuente de alimentación a través de Ethernet (PoE). Permite que los dispositivos de red reciban energía a través del cable de red mediante los mismos cables que las señales de datos. Todos los teléfonos IP H.323 compatibles en IP Office también admiten esta norma.

Cuando se va a instalar una gran cantidad de teléfonos, se recomienda usar conmutadores PoE. En el caso de otros escenarios, es posible usar dispositivos inyectores de PoE individuales para agregar compatibilidad para alimentación PoE a la conexión LAN del teléfono desde un conmutador que no es PoE.

Teléfonos IP H.323	Modelos compatibles	Clase PoE 802.3af	
		Clase	Desocupado
Serie 1600	1603	2	4,4W
	1603W	2	4,4W
	1608	2	3,7W
	1616	2	2,7W
Serie 9600	9608	1	2,08W
	9611G	1	2,8W
	9621G	2	3,49W
	9641G	2	3,44W

Estos teléfonos 1603 y 1603SW requieren una unidad separadora PoE aparte para poder utilizar PoE.

Si se excede el límite de clase de un puerto PoE o el respaldo de clase de un conmutador PoE puede producirse un funcionamiento incorrecto.

Tenga en cuenta que para los teléfonos que se utilizan con un módulo de botones de complementos y otros accesorios, hay más requisitos de alimentación. En el caso de los teléfonos 9608, 9611, 9621 y 9641, configure el interruptor de alimentación del teléfono en H y trate el teléfono como Clase 3.

Teléfonos de la serie 1600

Estos teléfonos pueden usar PoE como se ve arriba o pueden recibir alimentación mediante el uso de fuente de alimentación (PSU) con enchufe serie 1600. Existen diferentes modelos de

PSU para los diversos tipos de tomacorrientes eléctricos en diferentes países. La PSU se conecta al teléfono usando un conector de cilindro bajo el teléfono.

Teléfonos 9608, 9611, 9621 y 9641

Estos teléfonos solo admiten el conector Power over Ethernet (PoE). Si no se suministra con un conmutador PoE, puede usarse un inyector PoE de un solo puerto Avaya para cada teléfono.

Vínculos relacionados

Teléfonos IP Office H.323 en la página 10

Opciones de servidores de archivos

Durante la instalación y el mantenimiento, los teléfonos descargan varios archivos de firmware. Para ello, un teléfono primero solicita archivos para un servidor HTTPS. Si no recibe ninguna respuesta, luego intenta obtener los archivos a través de un servidor HTTP. La dirección para que use el servidor se proporciona como parte de la respuesta de DHCP que el teléfono recibió del servidor DHCP. Si se va a usar el sistema IP Office como el servidor DHCP, la dirección del servidor de archivos se configura como parte de la configuración de IP Office. Para teléfonos instalados mediante direcciones fijas, la dirección del servidor de archivos es una de las direcciones que se ingresó durante la instalación.

- Cada teléfono intentará solicitar archivos del servidor de archivos cada vez que se reinicia. Sin embargo, si el teléfono no recibe respuesta alguna, seguirá reiniciándose usando los archivos existentes que tiene en su propia memoria. Por lo tanto, no hay necesidad de que el servidor de archivos esté disponible de forma permanente después de la instalación inicial.
- Los teléfonos también emplean un servidor para la realización de copia de seguridad y restauración de la configuración del usuario durante el funcionamiento del teléfono. La dirección para este servidor se define mediante una configuración de dirección aparte que se encuentra en el archivo `46xxsettings.txt`. No es necesariamente el mismo servidor que se utiliza para los archivos de firmware del teléfono. Sin embargo, para el funcionamiento de IP Office, se recomienda usar la dirección del servidor IP Office como el servidor de archivos de copia de seguridad/restauración.

Las opciones que se detallan a continuación están disponibles para el servidor de archivos para los teléfonos IP que se estén instalando en un sistema IP Office.

Servidor de archivos	Hasta X teléfonos	TFTP (Puerto 69)	HTTP (Puerto 80)	HTTPS (Puerto 411)
IP Office Manager Cuando se encuentra en ejecución, IP Office Manager puede actuar como un servidor HTTP/TFTP para las solicitudes de archivos que se realicen desde teléfonos IP.	5	✓	✓	-

La tabla continúa…

Servidor de archivos	Hasta X teléfonos	TFTP (Puerto 69)	HTTP (Puerto 80)	HTTPS (Puerto 411)
Tarjeta de memoria IP500 V2 Para las unidades de control de IP Office equipadas con una tarjeta de memoria, esa tarjeta puede utilizarse para proporcionar los archivos de software. En el caso de unidades de control IP500 V2, la tarjeta del sistema es un elemento obligatorio y viene precargada con los archivos de firmware del teléfono durante la creación y actualizaciones de la tarjeta. Diversos otros archivos pueden generarse automáticamente por la unidad de IP Office si no existen en la tarjeta de memoria.	50	✓	✓	✓
Seleccione IP Office Server Edition/IP Office. Para sistemas IP Office, la aplicación IP Office puede actuar como el servidor de archivos. Los archivos de firmware del teléfono están instalados en el servidor como parte de la instalación de IP Office. Diversos otros archivos pueden generarse automáticamente por la unidad de IP Office si no existen en la tarjeta de memoria.	[1]	-	✓	✓
Software de terceros El software del servidor de archivos HTTP/TFTP de terceros está disponible a través de una gran cantidad de fuentes, incluso Avaya.	-	✓	✓	✓

[1] En una red IP Office Server Edition/IP Office Select, los servidores (distintos a una expansión IP500 V2) pueden actuar como servidor de archivos para la capacidad total de teléfonos del sistema. Sin embargo, la velocidad admitida para la entrega de firmware actualizado depende del tipo de servidor, como se indica a continuación. Si se necesita un rendimiento de actualización superior al indicado por las siguientes cifras, se puede usar un servidor de archivos HTTP/S externo.

- Dell R240: 100 teléfonos cada 50 minutos.
- HP DL360G7: 200 teléfonos cada 50 minutos.
- Dell R640: 300 teléfonos cada 50 minutos.
- OVA: hasta 300 teléfonos cada 50 minutos.

[2] En el caso de IP Office versión 9.0, para los sistemas IP Office que actúan como servidor de archivos, la redirección HTTP puede aplicarse para redirigir las solicitudes de teléfonos 9608, 9611, 9621 y 9641 de archivos .bin a un servidor HTTP por separado.

Vínculos relacionados

Teléfonos IP Office H.323 en la página 10

Tarjetas de memoria de la unidad de control

La tarjeta de memoria utilizada con los sistemas IP500 V2 puede utilizarse para almacenar archivos, incluso los utilizados por los teléfonos IP de Avaya.

La unidad de control IP500 V2 requiere todo el tiempo una tarjeta SD de sistema. Durante la creación de esta tarjeta, se coloca en la tarjeta un conjunto completo de archivos de firmware de IP Office incluyendo aquellos que usan los teléfonos IP de Avaya.

Prueba del servidor de archivos

Puede utilizar un navegador web para realizar una prueba básica del servidor de archivos. Por ejemplo, si utiliza HTTP, al escribir `http://<server_address>/46xxsettings.txt` debería aparecer el archivo `46xxsettings.txt`.

Si utiliza el sistema IP Office para generar automáticamente archivos, el archivo de configuración incluye texto donde se indica que el sistema lo generó automáticamente en respuesta a la solicitud del archivo. Esto es útil no solo para verificar la operación del servidor de archivos, sino también para ver la configuración que ofrece el sistema IP Office.

Vínculos relacionados

Teléfonos IP Office H.323 en la página 10

Solicitudes de archivos del teléfono

La mayoría de los teléfonos IP de Avaya, cuando se inician, atraviesan un proceso de solicitud de varios archivos de un servidor de archivos:

1. Generalmente, esto comienza con una solicitud de un archivo de actualización. Ese archivo indicará qué firmware debería estar ejecutándose en el teléfono. Si este es diferente al firmware que se está ejecutando, agregará los archivos de software que se enumeran a aquellos que va a descargar. La última línea del archivo de actualización le dice al teléfono el nombre del archivo de configuración que debería solicitar.
2. El teléfono solicita un archivo de configuración. Esto pasa una gran cantidad de archivos de configuración al teléfono. También puede enumerar archivos adicionales que el teléfono debe solicitar, como archivos de idioma y protectores de pantalla.
3. El teléfono solicita archivos adicionales:
   - Cualquier archivo de firmware que indique el archivo de actualización.
   - Cualquier archivo adicional que indique el archivo de configuración.
   - Cualquier archivo de configuración adicional.
4. Asimismo, el teléfono puede solicitar un archivo de configuración de usuario.

Lo antedicho es simplemente un resumen general. Según el tipo de teléfono, el orden de la solicitud de archivos puede variar. Además, si se solicita firmware para una actualización, el teléfono no puede solicitar otros archivos hasta que se haya completado la actualización del firmware y el teléfono se haya reiniciado.

Cuando el sistema IP Office se utiliza como servidor de archivos, tiene la capacidad de generar automáticamente muchos de los archivos que solicita el teléfono.

Vínculos relacionados

Teléfonos IP Office H.323 en la página 10
Generación automática de archivos en la página 27

Generación automática de archivos

Los teléfonos IP de Avaya solicitan un número de archivos del servidor de archivos cuando se reinicia el teléfono. Por ejemplo, archivos de firmware y configuración del teléfono.

Cuando se utiliza el sistema IP Office como servidor de archivos, cuando el teléfono solicita un archivo, si dicho archivo no está disponible, es posible que el sistema genere automáticamente un archivo. El archivo que se genera automáticamente utilizará una combinación de opciones y ajustes predeterminados de la configuración del sistema. Una vez suministrados al teléfono que lo solicite, el archivo generado automáticamente no se conserva en el sistema.

Esta característica se utiliza para casi todos los tipos de archivo, excepto para los archivos de firmware (por ejemplo, `.bin`, `.zip`, `.tar`) propiamente dichos y los archivos de certificados. Si un archivo propiamente dicho se carga en el sistema, se detiene la generación automática de ese archivo en particular.

Dentro del archivo `46xxsettings.txt` generado automáticamente:

- Los ajustes que se basan en entradas de configuración de IP Office, por ejemplo, configuración de idioma, aparecen en las secciones etiquetadas como "AUTOGENERATEDSETTINGS".
- Los ajustes que permanecen sin modificar para todos los sistemas IP Office que utilizan la misma versión de software aparecen en la sección etiquetada como "NONAUTOGENERATEDSETTINGS".

Prueba del servidor de archivos

Puede utilizar un navegador web para realizar una prueba básica del servidor de archivos. Por ejemplo, si utiliza HTTP, al escribir `http://<server_address>/46xxsettings.txt` debería aparecer el archivo `46xxsettings.txt`.

Si utiliza el sistema IP Office para generar automáticamente archivos, el archivo de configuración incluye texto donde se indica que el sistema lo generó automáticamente en respuesta a la solicitud del archivo. Esto es útil no solo para verificar la operación del servidor de archivos, sino también para ver la configuración que ofrece el sistema IP Office.

Vínculos relacionados

Solicitudes de archivos del teléfono en la página 26

Tarjeta de memoria de la unidad de control

La tarjeta de memoria utilizada con los sistemas IP500 V2 puede utilizarse para almacenar archivos, incluso los utilizados por los teléfonos IP de Avaya.

La unidad de control IP500 V2 requiere todo el tiempo una tarjeta SD de sistema. Durante la creación de esta tarjeta con IP Office Manager, se coloca en la tarjeta un conjunto completo de archivos de firmware de IP Office incluyendo aquellos que usan los teléfonos IP de Avaya.

Vínculos relacionados

Teléfonos IP Office H.323 en la página 10

Registro de listas negras

El sistema IP Office graba las solicitudes de registro H323/SIP fallidas. Varios intentos incorrectos pueden provocar que la extensión y/o la dirección IP se bloqueen por un tiempo.

El bloqueo se aplica de la siguiente manera:

Método	Descripción
Bloqueo de extensión	Los intentos para registrarse en una extensión existente con la contraseña incorrecta se bloquean durante 10 minutos después de 5 intentos fallidos en cualquier periodo de 10 minutos.
Bloqueo de dirección IP	Los intentos para registrarse en una extensión no existente o el uso de una contraseña incorrecta para una extensión existente se bloquean durante 10 minutos después de 10 intentos fallidos en cualquier periodo de 10 minutos.

Cuando se produce el bloqueo, el sistema genera una alarma en System Status Application y agrega una entrada a su registro de auditoría. También se genera una alarma del sistema, que puede transmitirse por cualquiera de las rutas de alarmas admitidas por el sistema (SMTP, SNMP, Syslog).

El monitor del sistema puede mostrar detalles de las direcciones IP y extensiones de la lista negra, seleccione **Estado** > **Estado y direcciones IP en lista negra** > **Extensiones bloqueadas**.

Vínculos relacionados

Teléfonos IP Office H.323 en la página 10

Bloqueo de claves predeterminadas

Acerca de esta tarea

Para IP Office R11.0 y superiores, la configuración de seguridad predeterminada bloquea el uso de claves de teléfono predeterminadas como 0000 para el registro de extensiones.

Procedimiento

1. Utilizando IP Office Manager, acceda a la configuración de seguridad del sistema.
2. En la ficha **General**, desactive la casilla de verificación **Bloquear códigos de acceso del teléfono IP predeterminados**.
3. Guarde la configuración.

Vínculos relacionados

Teléfonos IP Office H.323 en la página 10

Capítulo 2: Configuración adicional del teléfono

Los archivos de configuración `46xxsettings.txt` generados automáticamente son aptos para la mayoría de las instalaciones. Sin embargo, en algunos escenarios puede ser necesario modificar el valor de la configuración del archivo o agregar ajustes adicionales. Esto se puede hacer de diferente formas:

- **Usando archivos estáticos:** Reemplace el archivo generado automáticamente con un archivo real. Este método se recomienda únicamente para aquellos que tengan experiencia con la edición de archivos de configuración de teléfonos Avaya. El mayor inconveniente es que ya no se beneficiará con el cambio automático de ajustes para que coincidan con los cambios en la configuración de IP Office. Vea Configuración y edición de la configuración de archivos en la página 33.
- **Usar un archivo de configuración:** Si existe en el sistema un archivo denominado `46xxsettings.txt`, entonces el archivo `46xxsettings.txt` generado automáticamente le indica al teléfono que solicite ese archivo. Esto le permite cargar un archivo especial que contiene cualquier ajuste adicional o anular los ajustes seleccionados en el archivo generado automáticamente. Vea 46xxspecials.txt en la página 31.
- **Utilice números de origen NoUser:** Existe una cantidad de ajustes de número de origen NoUser que pueden utilizarse para agregar valores especiales al archivo de configuración generado automáticamente. Vea NoUser Source Numbers en la página 32.

Comandos adicionales comunes

Estos son algunos de los comandos adicionales más frecuentes. Si desea obtener todos los detalles de los comandos disponibles, consulte el manual del administrador de Avaya correspondiente para la serie de teléfonos en particular.

Descripción	Cómo configurar el comando de archivos
Password/CRAFT Configure la PROCPSWD que se especifica en el archivo `46xxsettings.txt` generado automáticamente, donde X es la contraseña. Esto es útil en escenarios como el funcionamiento de TLS que no puede habilitarse en teléfonos con PROCPSWD predeterminada.	`SET PROCPSWD X`
Contraseña de los administradores Configure la contraseña del administrador del teléfono Vantage que se especifica en el archivo `46xxsettings.txt` generado automáticamente donde X es la contraseña.	`SET ADMIN_PASSWORD X`

La tabla continúa…

Descripción	Cómo configurar el comando de archivos
Funcionamiento de los audífonos De manera predeterminada, los auriculares vuelven al estado colgado cuando la otra parte se desconecta. Al establecer este número de origen, este comportamiento se modifica de manera que los auriculares permanecen descolgados cuando la otra parte se desconecta.	`SET HEADSYS 1`
Temporizador de retroiluminación Establece el temporizador en minutos para el temporizador de retroiluminación del teléfono.	`SET BAKLIGHTOFF 60`

Protector de pantalla
Este conjunto de comandos
1. Habilite el protector de pantalla.
2. Configure el nombre del protector de pantalla para descargar.
3. Establece el nombre del archivo descargado actual que se utilizará.
	`SET SCREENSAVERON`
	`SET SCREENSAVER_IMAGE J179scr_svr.jpg`
	`SET SCREENSAVER_IMAGE_DISPLAY J179scr_svr`

Imagen de fondo Este conjunto de comandos 1. Configure el nombre de la imagen de fondo que desea descargar. 2. El nombre del archivo descargado actual que se utilizará.	`SET BACKGROUND_IMAGE J179bck_grnd.jpg` `SET BACKGROUND_IMAGE_DISPLAY J179bck_grnd`

Existen varios números de origen NoUser que se utilizan para extensión remota. Operan de manera diferente en el sentido de que cambian valores existentes en el archivo de configuración generado automáticamente dado a un teléfono cuando el sistema detecta que el teléfono que solicita el archivo es una extensión remota. Consulte el manual *"Teléfonos SIP IP Office con ABSCE"*.

Vínculos relacionados

46xxspecials.txt en la página 31
NoUser Source Numbers en la página 32
Configuración y edición de la configuración de archivos en la página 33

46xxspecials.txt

Para los sistemas que utilizan el archivo 46xxsettings.txt generado automáticamente, una opción para agregar la configuración manual adicional es utilizar un archivo llamado `46xxspecials.txt`. Cuando se agrega dicho archivo al sistema, el comando **`GET 46xxspecials.txt`** aparece como la última línea del archivo `46xxspecials.txt` generado automáticamente que solicitaron los teléfonos.

El archivo `46xxspecials.txt` debe crearse manualmente y luego colocarse en el servidor de archivos del teléfono. Puede ser:

- Archivo de texto simple que contiene un solo comando
- Archivo de configuración complejo con configuración basada en tipo de teléfono, modelo, grupo o modelo y grupo

Si desea obtener un ejemplo de una estructura compleja, puede navegar a `http://<IPOffice>/46xxspecials.txt` para obtener un archivo generado automáticamente. Guarde y edite ese archivo antes de volver a cargarlo en el sistema.

Vínculos relacionados

Configuración adicional del teléfono en la página 30

NoUser Source Numbers

Most values in the auto-generated settings file are based on settings taken from the IP Office system configuration. However, it may occasionally be necessary to add additional values to the auto-generated files. This can be done using the values entered as `NoUser` source numbers.

- Since these changes are applied to the values in the auto-generated `46xxsettings.txt` file, they are overridden by any setting entered in the `46xxsettings.txt` file if present.
- There are a number of **NoUser** source number settings used for remote extensions. They operate differently in that they change existing values in the auto-generated settings file given to a phone when the system detects that the phone requesting the file is a remote extension. Refer to the IP Office SIP Phones with ASBCE manual.

Example NoUser Source Numbers

	Description
`SET_46xx_PROCPSWD=X`	This NoUser source number adds the command **`SET PROCPSWD X`** to the auto-generated settings file where **`X`** is the password set.
`SET_ADMINPSWD=X`	This NoUser source number adds the command **`SET ADMINPSWD X`** to the auto-generated settings file where **`X`** is the password set.
`SET_HEADSYS_1`	This NoUser source number adds the command **`SET ADMINPSWD X`** to the auto-generated settings file.
`SET_BAKLIGHTOFF=N`	This NoUser source number adds the command **`SET BAKLIGHTOFF N`** to the auto-generated settings file provided to a remote extension. **`N`** is the timeout in minutes.

Related links

Configuración adicional del teléfono on page 30

Configuración y edición de la configuración de archivos

Acerca de esta tarea

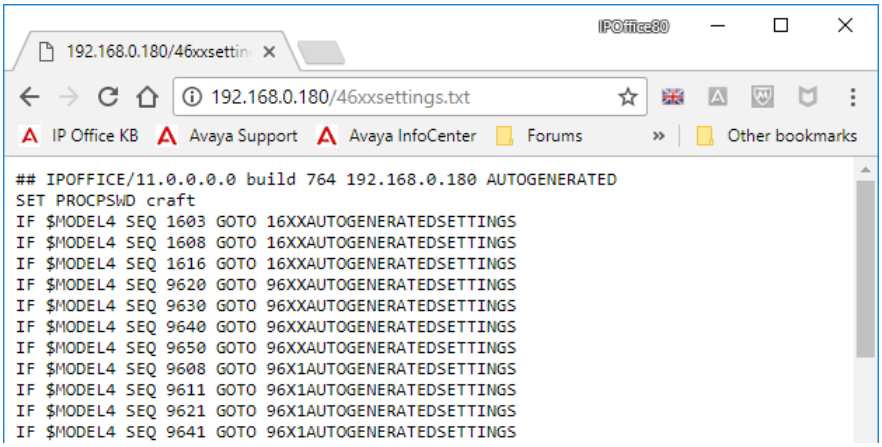
La mayoría de los teléfonos IP Avaya descargan un archivo de configuración al reiniciarse. Este archivo contiene un rango de opciones.

Nota:

Siempre que sea posible utilice el sistema IP Office como servidor de archivos y deje que genere automáticamente los archivos de configuración. Esto ayuda a que el sistema ajuste automáticamente las opciones proporcionadas a los teléfonos para que coincidan con los cambios realizados en la configuración del sistema.

Procedimiento

1. Desplácese hasta el sistema e introduzca el nombre del archivo de configuración del teléfono específico requerido, por ejemplo, http://192.168.42.1/46xxsettings.txt. El archivo generado automáticamente aparece en el navegador.



   - En la mayoría de los teléfonos: `46xxsettings.txt`
   - Serie 1100/1200: `11xxsettings.txt`
   - H175: `H1xxsettings.txt`

2. Guarde el archivo como archivo de texto local.
   - Para guardar el archivo con el navegador Chrome, haga clic con el botón secundario en la ventana y seleccione **Guardar como**.
   - Para guardar el archivo con el navegador Explorer, seleccione **Archivo** > **Guardar como**.
   - Para guardar el archivo con el navegador Firefox, seleccione **Guardar página como**.

   El archivo descargado ahora puede editarse con un editor de texto. Los campos admitidos se describen en el manual de administración correspondiente para la serie del teléfono.
3. Al finalizar, cargue el archivo al servidor de archivos que utilizan los teléfonos.
4. Reinicie el o los teléfonos para que puedan volver a cargar sus archivos, incluida la descarga del archivo de configuración editado.

Vínculos relacionados

Configuración adicional del teléfono en la página 30

Parte 2: Proceso básico de instalación

Instalación del teléfono IP H.323

El siguiente es un resumen de pasos importantes en el proceso de instalación. El método de instalación recomendado es utilizar DHCP cuando sea posible, usar el sistema IP Office como el servidor de archivos y activar la creación automática de usuarios y extensiones.

	Descripción
PC que ejecuta la aplicación Manager:	Compruebe que IP Office Manager, System Status Application y System Monitor estén instalados y puedan utilizarse para conectarse al sistema IP Office. Verifique que pueda recibir la configuración del sistema y vuelva a enviarla.
Canales de compresión de voz	En el caso de los sistemas IP500 V2, la unidad de control debe contar con canales de compresión de voz. Utilice la aplicación System Status Application (SSA) o System Monitor para verificar que los canales de compresión de voz estén disponibles. SSA enumera los canales de módulos de compresión de voz (VCM) en la pantalla **Recursos**. Las líneas iniciales de la salida de Monitor incluyen el elemento VCOMP= que establece la cantidad de canales instalados en la unidad de control.
Licencias o suscripciones	Dependiendo del modo operativo del sistema, cada teléfono requiere una licencia o suscripción. Los teléfonos pueden registrarse sin una licencia o suscripción, pero no funcionarán. Vea Licencias y suscripciones en la página 17.
Configuración de Gatekeeper de H.323	El sistema IP Office es compatible para teléfonos H.323 activados de forma predeterminada. Sin embargo, esto debe verificarse.
Configuración de servidor DHCP	DHCP es el método recomendado para instalar teléfonos IP en un sistema IP Office. Para esto se requiere un servidor DHCP configurado para que sea compatible con teléfonos IP. El sistema IP Office puede utilizarse para esto. Si el cliente desea usar su propio servidor DHCP, requiere una configuración adicional.
Configuración de servidor de archivos de teléfono	Si se va a usar el sistema IP Office para DHCP, también es necesario configurarlo con la dirección del servidor de archivos. Cualquiera sea el método de instalación y el servidor de archivos que se seleccione, deben agregarse los archivos de firmware del sistema a los archivos disponibles en el servidor.

La tabla continúa…

	Descripción
Configuración de extensiones y usuarios	El sistema IP Office puede configurarse para que cree automáticamente entradas de usuarios y extensiones en su configuración para cada teléfono IP que esté instalado. Si no se utiliza la creación automática, es necesario crear manualmente las entradas para cada extensión y usuario antes de que se instalen los teléfonos.
Conexiones de los teléfonos	Una vez completados los pasos anteriores, se pueden conectar los teléfonos a la red. Si se va a usar DHCP, los teléfonos obtendrán automáticamente información de la dirección IP y otras configuraciones y luego comenzarán la carga de archivos. Si no se va a usar DHCP, será necesario realizar un proceso manual en los teléfonos para ingresar la información y configuración de direcciones IP.
Registro del teléfono	Una vez que los teléfonos han descargado todos los archivos que necesitan del servidor de archivos, intentarán registrarse con el sistema IP Office. Los teléfonos indicarán la entrada del número de extensión que se debe usar.
Prueba	Debe probarse el funcionamiento de los teléfonos haciendo varias llamadas, como llamadas externas.
Postinstalación	Si se utilizó Creación automática para entradas de usuarios y/o extensiones, dicha configuración debe desactivarse después que se concluya con la instalación de todos los teléfonos. Este manual solo detalla la configuración mínima de usuario que se requiere para la instalación. Los nuevos usuarios ahora pueden configurarse completamente para que atiendan los requisitos de otros usuarios.

Capítulo 3: Licencias y suscripciones

Suscripciones

Los sistemas que se ejecutan en modo de suscripción admiten extensiones hasta la cantidad total de suscripciones de usuario disponibles.

Licencias

Para sistemas que no se ejecutan en modo de suscripción, se requieren licencias para cada extensión IP.

- En sistemas IP Office Server Edition, el usuario debe estar configurado con un perfil de usuario con licencia, como una licencia de Usuario básico. Los usuarios sin licencia no pueden iniciar sesión en una extensión.
- Para teléfonos Avaya, se requiere una licencia Avaya IP Endpoint para cada teléfono. Esto incluye todos los teléfonos 1600, 9600, IP DECT, DECT R4 y Spectralink.
- Para teléfonos IP que no son de Avaya, se requiere una licencia para terminal IP de terceros.
  - De forma predeterminada, cada teléfono IP de Avaya que se registra en el sistema IP Office utiliza una licencia, siguiendo el orden en que se registran. La licencia queda liberada cuando el teléfono registra su salida. No obstante, es posible reservar una licencia para determinados teléfonos y así garantizar que esos teléfonos siempre obtengan una. Esto se realiza a través de la configuración **Reservar licencia de terminal IP de Avaya** de cada extensión IP. En sistemas que utilizan concesión de licencias WebLM, esta opción está fija para reservar una licencia.
  - Los teléfonos Avaya IP sin una licencia aún pueden registrarse pero están limitados a realizar únicamente llamadas de emergencia (llamadas de código corto Marcar emergencia). El usuario vinculado se considera desconectado, y el teléfono muestra el mensaje "No license available" (Sin licencia disponible). Si hay disponible una licencia, se asigna a cualquier auricular DECT sin licencia primero y luego a cualquier otro teléfono Avaya sin licencia en el orden en el que los teléfonos se hayan registrado.

Vínculos relacionados

Teléfonos IP Office H.323 en la página 10
Reserva de licencias en la página 37

Reserva de licencias

Acerca de esta tarea

Este proceso particular no puede realizarse normalmente hasta que se haya creado la entrada de la extensión. Si se va a usar creación de extensiones automática (lo predeterminado), esto significa que no es posible realizar reservación de licencia hasta después de la instalación inicial del teléfono. Sin embargo, debería considerarse el uso de esta configuración con

teléfonos existentes que ya están instalados a fin de asegurar que en lo posible conserven sus licencias después de la adición de otros teléfonos.

Normalmente, las licencias se asignan a las extensiones de manera automática en el orden de registro. Sin embargo, las extensiones actuales pueden reservar una licencia para garantizar que no se queden sin licencia cuando se logren registrar nuevas extensiones agregadas al sistema después de un reinicio del sistema.

- En sistemas que utilizan concesión de licencias WebLM, esta opción está fija para reservar una licencia.
- La reserva de licencias no es compatible con sistemas en modo de suscripción.

Procedimiento

1. Utilizando IP Office Manager, reciba la configuración del sistema del teléfono.
2. Seleccione **Extensión** y después seleccione la extensión de H.323.
3. Seleccione la ficha **VoIP**.
4. Configure el campo **Reservar licencia** en **Reservar licencia de terminal IP de Avaya**.
5. Repita el proceso para cualquier otra extensión para la cual desea reservar la licencia.
6. Guarde la configuración.

Vínculos relacionados

Licencias y suscripciones en la página 17

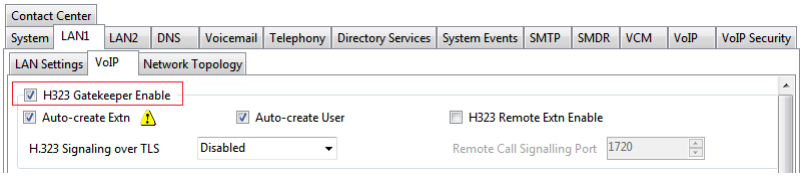
Capítulo 4: Activación del gatekeeper de H.323

Acerca de esta tarea

La compatibilidad para teléfonos y líneas H.323 viene activa de forma predeterminada. Sin embargo, esto debe verificarse.

Procedimiento

1. Utilizando IP Office Manager, recupere la configuración del sistema.
2. Seleccione **SISTEMA**.
3. Seleccione la ficha **LAN1** o **LAN2** según la interfaz LAN del sistema que desee usar para admitir las extensiones H.323.
4. Seleccione la subficha **VoIP**.



5. Utilice la casilla de verificación de configuración de **Habilitar Gatekeeper de H323**.
6. Guarde la configuración.

Vínculos relacionados

Configuración del intervalo de puertos RTP en la página 39
Ajuste de la QoS de DiffServ en la página 41
Códecs predeterminados del sistema en la página 41

Configuración del intervalo de puertos RTP

Acerca de esta tarea

Los puertos usados para llamadas VoIP H.323 varían para cada llamada. El intervalo para los puertos usados puede ajustarse a fin de evitar conflictos con otros servicios. Si el cliente tiene firewalls internos o equipos similares que apliquen filtros a los puertos o que solo remite tráfico de acuerdo al puerto que se use, el intervalo que se establezca debe estar permitido por esos dispositivo.

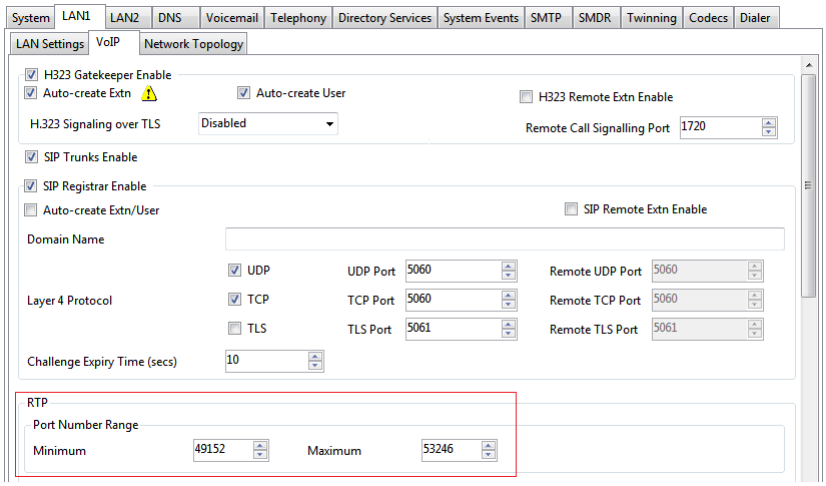
Para cada llamada VoIP, los puertos que reciben se seleccionan del intervalo que se define más abajo. Los números pares en el intervalo se usan para el tráfico de llamadas entrantes

del Protocolo en tiempo real (RTP). El tráfico del Protocolo de control en tiempo real (RTCP) de la misma llamada utiliza el número de puerto RTP más 1, es decir, los números impares.

Se recomienda utilizar sólo números de puerto mayores o iguales a 49152 pero estrictamente menores a 65535, ya que ese es el intervalo definido por la Autoridad de números asignados de Internet (IANA) para el uso dinámico.

Procedimiento

1. Utilizando IP Office Manager, recupere la configuración del sistema.
2. Seleccione **SISTEMA**.
3. Seleccione la ficha **LAN1** o **LAN2** según la interfaz LAN del sistema que desee usar para admitir las extensiones H.323.
4. Seleccione la subficha **VoIP**.



5. Verifique el **Intervalo de números de puerto**que se muestra en la sección **RTP**. Recuerde que el tráfico RTCP coincidente usa el mismo intervalo más 1.
   - **Mínimo**: Predeterminado = 49152. Rango = 1024 a 65280.

     Esto configura el límite inferior de los números de puerto RTP utilizados por el sistema. La elección de un intervalo mínimo de menos de 1024 solo debe hacerse después de realizar un cuidadoso análisis de la configuración total.
   - **Máximo**: Predeterminado = 53246. Rango = 1278 a 65534.

     Esto configura el límite superior de los números de puerto RTP utilizados por el sistema. El intervalo entre el mínimo y el máximo debe ser de al menos 254. La elección de un intervalo mínimo de menos de 1024 solo debe hacerse después de realizar un cuidadoso análisis de la configuración total.
6. Guarde la configuración.

Vínculos relacionados

Activación del gatekeeper de H.323 en la página 39

Ajuste de la QoS de DiffServ

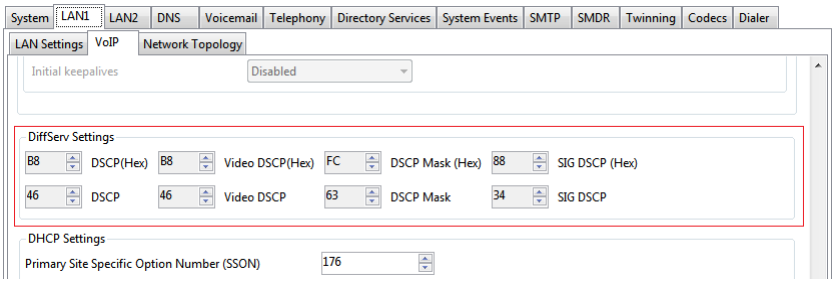
Acerca de esta tarea

DiffServ se utiliza para aplicar diferentes etiquetas de "calidad de servicio" a los elementos de voz (RTP) y señal de control (RTCP) de una llamada de VoIP. El sistema IP Office en sí no aplica ninguna prioridad diferente a los paquetes de datos que recibe o envía basándose en sus etiquetas. Sin embargo, cuando se va a usar en una red donde otros dispositivos emplean la QoS para otorgar prioridad, la configuración de IP Office se debe establecer de forma que coincida con la configuración esperada para llamadas de voz y sus señales de control

relacionadas.

Procedimiento

1. Utilizando IP Office Manager, recupere la configuración del sistema.
2. Seleccione **SISTEMA**.
3. Seleccione la ficha **LAN1** o **LAN2** según la interfaz LAN del sistema que desee usar para admitir las extensiones H.323.
4. Seleccione la subficha **VoIP**.



   Verifique los **Configuración ServDif** que usa el sistema. Tenga en cuenta que las dos filas están relacionadas, la superior muestra los valores de DiffServ en números hexadecimales y la inferior, en decimales. Los valores hexadecimales son iguales a los decimales multiplicados por 4. Cada fila puede usarse para configurar los valores necesarios.

5. Guarde la configuración.

Vínculos relacionados

Activación del gatekeeper de H.323 en la página 39

Códecs predeterminados del sistema

Acerca de esta tarea

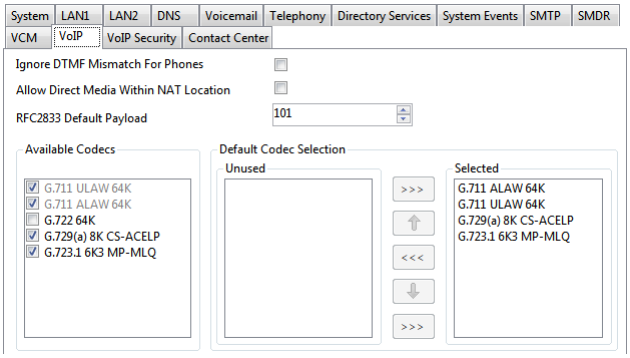
De manera predeterminada, todos los dispositivos VoIP que se añaden a la configuración de IP Office usan las preferencias de códec predeterminas del sistema. Esto se muestra en la configuración de **Códec** en una línea troncal IP o extensión que se configura como **Predeterminado del sistema**.

Además, para cambiar el orden predeterminado de preferencia de códecs para todas las extensiones y troncales VoIP, es posible ajustar las preferencias de códecs usadas por una

troncal o extensión en particular. Sin embargo, al usar la configuración común del sistema se asegura la uniformidad de códecs entre troncales y extensiones.

Procedimiento

1. Utilizando IP Office Manager, recupere la configuración del sistema.
2. Seleccione **SISTEMA**.
3. Seleccione la subficha **VoIP**.



La sección Selección predeterminada se utiliza para configurar el orden predeterminado de preferencia de códecs. Esto lo usan todas las extensiones y líneas IP (H.323 y SIP) del sistema que tienen las opciones de **Selección de códec** configuradas en **Predeterminado del sistema**. Estas son las opciones predeterminadas para todas las líneas y extensiones IP agregadas.

La lista **Códecs disponibles** muestra qué códecs admite el sistema. Los códecs de esta lista que están activados son aquellos que pueden usarse en otros formularios de configuración, incluida la selección predeterminada adyacente.

Advertencia:

Al quitar la selección de un códec en esta lista, se lo elimina automáticamente de cualquier lista de códecs de línea o extensión donde se estaba usando.

4. Guarde la configuración.

Vínculos relacionados

Activación del gatekeeper de H.323 en la página 39

Capítulo 5: Configuración de DHCP

La recomendación para la instalación del teléfono H.323 es usar DHCP, en especial si se va a instalar una gran cantidad de teléfonos. El uso de DHCP simplifica tanto la instalación como el mantenimiento. Existen varias opciones para las cuales se usa servidor para compatibilidad con DHCP para los teléfonos H.323:

- Si se va a utilizar el sistema IP Office como servidor DHCP para la red, utilice los procesos a continuación para verificar y configurar las opciones de DHCP del sistema.
- Si la red del cliente usa un servidor DHCP aparte, es posible que el servidor DHCP deba configurarse para admitir solicitudes DHCP de teléfonos IP.
- IP Office puede configurarse para brindar compatibilidad DHCP solo para teléfonos Avaya. Esa opción puede seleccionarse para poder utilizarse en conjunto con un servidor DHCP de cliente aparte. Esto elimina la necesidad de configurar el servidor DHCP del cliente para que admita teléfonos IP.

Advertencia:

- Si se activa un servidor DHCP adicional en una red se pueden producir problemas de conexión para todos los dispositivos de la red. Asegúrese de que usted, el usuario, y el administrador de la red del usuario acepten todos la elección correcta de la opción de servidor DHCP.

Vínculos relacionados

Compatibilidad con DHCP del sistema en la página 43
Números de opción específicos del sitio del sistema en la página 44
Cambio de la configuración del SSON del sistema en la página 44

Compatibilidad con DHCP del sistema

Procedimiento

1. Utilizando IP Office Manager, recupere la configuración del sistema.
2. Seleccione **SISTEMA**.
3. Seleccione la ficha **LAN1** o **LAN2** según la interfaz LAN del sistema que desee usar para admitir las extensiones H.323.
4. Seleccione la ficha **Configuración de LAN**.
5. En **Número de direcciones IP de DHCP**, configure el valor para el número de direcciones IP que el sistema puede emitir.
6. En **Modo DHCP**, seleccione **Servidor**.

7. Haga clic en **Avanzada**. La configuración de **Avanzada** permite ajustar la configuración **DHCP**, incluido el agregado de diversos intervalos de números **DHCP** que puede admitir el sistema IP Office. Tenga en cuenta que los intervalos de dirección fuera de aquellos de la subred propia de sistemas también pueden requerir la creación de rutas IP adecuadas para garantizar el enrutamiento de tráfico entre las subredes.

   Nota:

   - Los cambios a grupos DHCP no requieren un reinicio del sistema IP Office. Sin embargo, provoca el reinicio de los teléfonos H323 y SIP Avaya conectados al sistema. Los teléfonos que no sean de Avaya no se reiniciarán, pero deberán reiniciarse manualmente para obtener una dirección válida de la configuración de grupos nuevos.

   Seleccione la casilla de verificación **Aplicar solo al teléfono IP de Avaya**.

   IP Office actúa como servidor DHCP solo para teléfonos Avaya. Esta opción no puede emplearse si también se admiten teléfonos de las series 1100 y 1200.

8. Guarde la configuración.

Vínculos relacionados

Configuración de DHCP en la página 43

Números de opción específicos del sitio del sistema

Cuando se solicita configuración de dirección de un servidor DHCP, cada teléfono también solicita información adicional que pueda tener el servidor DHCP. Para ello, envía un número de opción específico del sitio (SSON). Si el servidor DHCP tiene información que coincida con el SSON, dicha información se incluye en la respuesta DHCP.

Los teléfonos de la serie 1600 y 9600 usan 242 como su SSON predeterminado. Sin embargo, a través de los propios menús del teléfono, es posible alterar el SSON que usa. Para aquellos teléfonos que emplean el sistema IP Office para DHCP, los números SSON que admite IP Office están establecidos en la configuración del sistema IP Office. Los valores que usan los teléfonos y que son compatibles con el sistema IP Office deben coincidir.

Vínculos relacionados

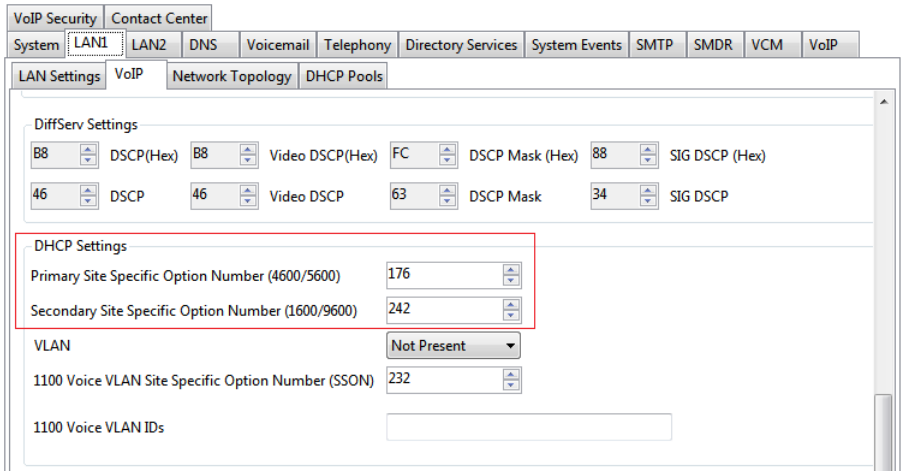
Configuración de DHCP en la página 43

Cambio de la configuración del SSON del sistema

Procedimiento

1. Utilizando IP Office Manager, recupere la configuración del sistema.
2. Seleccione **SISTEMA**.
3. Seleccione la ficha **LAN1** o **LAN2** según la interfaz LAN del sistema que desee usar para admitir las extensiones H.323.

4. Seleccione la subficha **VoIP**.



5. Verifique que la configuración del número de opción específico del sitio coincida con la que se requiere para los teléfonos compatibles. El valor predeterminado para los teléfonos de las series 1600 y 9600 es 242.
6. Guarde la configuración.

Vínculos relacionados

Configuración de DHCP en la página 43

Capítulo 6: Configuraciones del servidor de archivos

Como parte del proceso de instalación, el teléfono solicita archivos de un servidor de archivos. Con DHCP, la dirección del servidor de archivos se obtiene como parte de la respuesta de DHCP desde el servidor DHCP. Se ingresa la dirección del servidor de archivos en el teléfono como parte del proceso de direcciones fijas.

Las opciones de servidor de archivos son:

- Para sistemas IP500 V2, puede utilizarse la tarjeta de memoria del propio sistema IP Office como fuente para los archivos. Esta es la opción recomendada y puede usarse para hasta 50 teléfonos.
- Para sistemas IP Office Server Edition, puede utilizarse el disco propio del sistema como fuente para los archivos que utilizan los teléfonos para la capacidad total de teléfonos admitidos del sistema.
- Puede utilizarse redirección HTTP para permitir que un servidor por separado proporcione los archivos binarios para los teléfonos 9608, 9611, 9621 y 9641 mientras que el sistema IP Office proporciona todos los demás archivos.
- La aplicación IP Office Manager también puede actuar como un servidor de archivos para hasta cinco (5) teléfonos. Si las opciones anteriores no son aceptables o no coinciden con las necesidades de capacidad del sistema, se necesita un servidor de archivos HTTP externo. Deben cargarse los archivos de firmware de teléfono necesarios en ese servidor.

Uso de puertos

El puerto usado por teléfono IP para solicitar archivos depende del tipo de teléfono.

Puerto	Utilización	Teléfonos
80	No seguro: firmware, configuración y datos del usuario del teléfono.	Todos
411	Seguro: configuración, datos del usuario.	Teléfonos H.323 9608, 9611, 9621 y 9641
443	Seguro: firmware, configuración y datos del usuario del teléfono.	Teléfonos SIP
8411	No seguro: firmware del teléfono.	Teléfonos remotos H.323

En los teléfonos más nuevos, se puede indicar qué puerto se usará a través de la respuesta DHCP o del archivo de configuración proporcionado inicialmente al teléfono. Si no hay respuesta en ese puerto, es posible que el teléfono recurra como reserva a uno de los valores de puerto predeterminados. Sin embargo, algunos teléfonos más antiguos están codificados de forma rígida para usar puertos fijos.

Vínculos relacionados

Cambio de las configuraciones del servidor de archivos en la página 47

Cambio de las configuraciones del servidor de archivos

Acerca de esta tarea

Si se emplea el sistema IP Office para compatibilidad DHCP para los teléfonos IP, se utilizan diversas opciones en el sistema IP Office para configurar las direcciones del servidor de archivos que se envían a los teléfonos en las respuestas DHCP.

Procedimiento

1. Utilizando IP Office Manager, recupere la configuración del sistema.
2. Seleccione **SISTEMA**.
3. Seleccione la ficha **SISTEMA**.
4. Compruebe la configuración de **Tipo de servidor de archivos de teléfonos**. Vea Configuración del servidor de archivos del teléfono en la página 48.
5. En **Tipo de servidor de archivos de teléfonos**, establezca la configuración según sea necesario. Consulte Configuración del servidor de archivos del teléfono en la página 48 para obtener detalles de las diferentes configuraciones utilizables.
6. Para los teléfonos 9608, 9611, 9621 y 9641, seleccione la opción **Redirección HTTP** que se puede utilizar para enviar solicitudes de archivos binarios del teléfono al **Dirección IP del servidor HTTP** por separado.
7. Habilite la casilla de verificación **Utilizar puertos telefónicos preferidos** para reducir el uso de los puertos HTTP/HTTPS configurados en la configuración de seguridad del sistema (de manera predeterminada, los puertos 80 y 443) para las solicitudes de archivos del teléfono.
   - Cuando la casilla de verificación está habilitada **Utilizar puertos telefónicos preferidos**, los archivos de configuración de teléfono generados automáticamente para teléfonos locales indican el puerto 8411 para HTTP y 411 para TLS.
   - Cuando la casilla de verificación **Utilizar puertos telefónicos preferidos** está desactivada, los archivos de configuración de teléfono generados automáticamente proporcionados por el sistema a los teléfonos locales indican los puertos 80/411 u 80/443, según el tipo de teléfono.

     Los archivos de configuración de teléfono generados automáticamente proporcionados por el sistema a los teléfonos remotos indican los puertos 8411/411 u 8411/443, según el tipo de teléfono.

8. Habilite la casilla de verificación **Solo clientes HTTP de Avaya** para restringir el sistema para que solo responda a las solicitudes del archivo de teléfonos y aplicaciones Avaya.

   Nota:

   Esta opción no debe usarse si el sistema también va a admitir teléfonos de la serie 1100 o 1200.

9. Guarde la configuración.

Vínculos relacionados

Configuraciones del servidor de archivos en la página 46

Configuración del servidor de archivos del teléfono

Los siguientes ajustes se utilizan para los teléfonos H323 que solicitan archivos de firmware del sistema IP Office:

Campo	Descripción
Tarjeta de memoria (IP500 V2) **Disco** (IP Office Server Edition)	Utilice la memoria del sistema. La dirección IP del sistema se proporciona como valores del servidor de archivos TFTP y HTTP en la respuesta DHCP. Esta es la configuración predeterminada.
Manager	Utilice la aplicación IP Office Manager como el servidor de archivos TFTP y HTTP. Esta opción solo es compatible para un máximo de 5 teléfonos IP. Esta opción utiliza la Dirección IP de PC Manager aparte que se establece en la configuración. El sistema usa el valor predeterminado 0.0.0.0 para difundir cualquier aplicación IP Office Manager disponible que se esté ejecutando en la red. Tenga en cuenta que, de manera predeterminada, la opción IP Office Manager para la compatibilidad con TFTP está deshabilitada (**Archivo** > **Preferencias** > **Preferencias** > **Habilitar servidores BootP y TFTP**).
Personalizar	Esta opción usa los valores aparte Dirección IP del servidor TFTP y Dirección IP del servidor HTTP establecidos en la configuración como las direcciones de servidor de archivos en la respuesta DHCP que se entrega a los teléfonos.

Vínculos relacionados

Configuraciones del servidor de archivos en la página 46

Creación/edición del archivo de configuración

Durante la instalación, los teléfonos solicitan archivos que primero descargan un archivo xxupgrade del servidor de archivos. Luego, siguen las instrucciones dentro de ese archivo para solicitar más archivos de ser necesario. Existen diversos archivos xxupgrade diferentes para las distintas series de teléfonos. Estos se proporcionan como parte del firmware del teléfono. Los archivos xxupgrade no deben editarse o cambiarse de ninguna forma.

La última línea de todos los archivos xxupgrade ordenan a los teléfonos que soliciten el archivo `46xxsettings.txt`. Este archivo puede emplearse para establecer configuraciones específicas del sitio para todos los teléfonos IP Avaya H.323 que se admitirán en un sitio en particular.

Al usar el sistema IP Office como el servidor de archivos, el sistema IP Office creará automáticamente un archivo `46xxsettings.txt` adecuado en diversas configuraciones del sistema IP Office. Solo hará esto si no hay un archivo `46xxsettings.txt` actual disponible en el servidor.

Prefijo de marcado

En sistemas IP Office, la incorporación o eliminación de prefijos de marcado es realizada por el sistema IP Office en lugar de los teléfonos individuales. No se admite el uso de reglas de marcado mejoradas a través del archivo de configuración del teléfono.

Etiquetado 802.1Q

A menos que se requiera específicamente para la red del cliente, para el funcionamiento de IP Office se recomienda cambiar ## SET L2Q 0 a SET L2Q 2.

Idiomas de los teléfonos de las series 1600 y 9600

Además del inglés, los teléfonos de las series 1600 y 9600 son compatibles con hasta otros cuatro (4) idiomas. Esto lo realizan los teléfonos, que descargan los archivos de idiomas especificados en el archivo `46xxsettings.txt`. En la actualidad, se proporcionan nueve (9) archivos de idiomas que no son inglés como parte de la instalación de IP Office Manager.

Idioma	Archivo de 1600	Archivo de 9600
Turco	mlf_dutch.txt	mlf_9600_dutch.txt
Francés (Canadá)	mlf_french_can.txt	mlf_9600_french_can.txt
Francés	mlf_french_paris.txt	mlf_9600_french_paris.txt
Alemán	mlf_german.txt	mlf_9600_german.txt
Italiano	mlf_italian.txt	mlf_9600_italian.txt
Portugués	mlf_portuguese.txt	mlf_9600_portuguese.txt
Ruso	mlf_russian.txt	mlf_9600_russian.txt
Español	mlf_spanish.txt	mlf_9600_spanish.txt
Español (América Latina)	mlf_spanish_latin.txt	mlf_9600_spanish_latin.txt

Los archivos para descargar en los teléfonos se definen en las secciones `# SETTINGS1603`, `# SETTINGS1608` y `# SETTINGS1616` del archivo `46xxsettings.txt`. Para que el teléfono descargue un archivo de idioma, elimine ## de la parte delantera de una de las opciones `SET` y cambie el nombre del archivo para que coincida con el idioma requerido. Si se va a utilizar el sistema IP Office como el servidor de archivos, pueden proporcionarse archivos de idioma adecuados basados en la configuración del sistema IP Office usando la generación automática de archivos.

Copia de seguridad/restauración

Los teléfonos pueden utilizar un servidor HTTP como una ubicación para guardar una copia de seguridad y restaurar la configuración del teléfono del usuario al iniciar o cerrar sesión en él. Consulte configuraciones de copia de seguridad/restauración en la página 67 para obtener todos los detalles.

Protector de pantalla

Puede especificar la cantidad de minutos que desea que transcurran antes de que un teléfono inactivo muestre un protector de pantalla y el nombre del archivo de imagen. Vea Protector de pantalla en la página 65.

Vínculos relacionados

Configuraciones del servidor de archivos en la página 46

Edición manual del archivo

Procedimiento

1. Ubique el archivo `46xxsettings.txt` en el servidor de archivos.
2. Abra el archivo `46xxsettings.txt` con un editor de texto sin formato.
3. Edite el archivo conforme sea necesario.

   El archivo contiene una gran cantidad de comentarios y notas. En el Manual del administrador de LAN Avaya apropiado puede obtener más detalles sobre las diversas configuraciones según el tipo de teléfono. Tenga en cuenta que los archivos tienen una amplia gama de configuraciones usadas en otros sistemas de teléfonos Avaya que no necesariamente funcionen o sean compatibles con los sistemas IP Office.

   El carácter # al principio de una línea es el comando de esa línea.

Vínculos relacionados

Configuraciones del servidor de archivos en la página 46

Carga de archivos de software en el sistema

En el caso de los sistemas IP Office Server Edition, el firmware del teléfono adecuado para el funcionamiento del sistema IP Office se incluye como parte de la instalación del sistema IP Office en el servidor. Por lo tanto, no se requiere ninguna otra acción si se va a usar el sistema como servidor de archivos para instalación del teléfono. El firmware también se incluye como parte de IP Office Manager y se copia en la computadora cuando IP Office Manager está instalado. No se debe usar otro firmware con IP Office a menos que esté específicamente documentado. El firmware instalado puede verificarse y es posible copiar nuevo firmware en el disco del sistema del teléfono si es necesario.

El firmware del teléfono adecuado para el funcionamiento del sistema IP Office se suministra como parte del software IP Office Manager y se copia en la PC cuando se instala IP Office Manager. No se debe usar otro firmware con IP Office a menos que esté específicamente documentado.

Hay varios métodos mediante los cuales el firmware instalado con IP Office se puede copiar a la tarjeta de memoria del sistema del teléfono. El método depende principalmente del tipo de unidad de control.

⚠ Advertencia:

- La tarjeta de memoria no se debe quitar nunca de un sistema en ejecución sin apagar primero la tarjeta o el sistema. IP Office Manager se debe usar para apagar la tarjeta de memoria antes de quitarla del sistema.
- Para el funcionamiento de IP Office, solo los archivos .bin del teléfono tienen que estar presentes en la tarjeta de memoria. Otros archivos que requieren los teléfonos los genera automáticamente el sistema en respuesta a las solicitudes de los teléfonos.

Vínculos relacionados

Configuraciones del servidor de archivos en la página 46

Unidad de control IP500 V2

La tarjeta SD del sistema se usa para almacenar los archivos. Esta es una tarjeta obligatoria que está presente en todos los sistemas IP500 V2. Los archivos de firmware se cargan en la tarjeta de distintas maneras:

- Si el sistema se actualizó usando la opción **Recrear tarjeta SD** en IP Office Manager, el firmware se copia automáticamente en la tarjeta como parte de ese proceso.
- Si el sistema se actualizó con el Asistente de actualización de IP Office Manager, y la opción **Cargar archivos de sistema** estaba seleccionada, el firmware se copiará a la tarjeta como parte de ese proceso. De forma predeterminada, la opción **Cargar archivos de sistema** está habilitada.

Si piensa que los archivos correctos no están presentes, puede usar el administrador de archivos integrado, que es parte de IP Office Manager, para verificar los archivos en la tarjeta y copiarlos a esta de ser necesario.

Vínculos relacionados

Configuraciones del servidor de archivos en la página 46

Uso del Administrador de archivos integrados para verificar/cargar archivos

Acerca de esta tarea

El administrador de archivos integrado le permite ver de modo remoto los archivos de la tarjeta de memoria que utiliza el sistema del teléfono. También le permite cargar archivos nuevos.

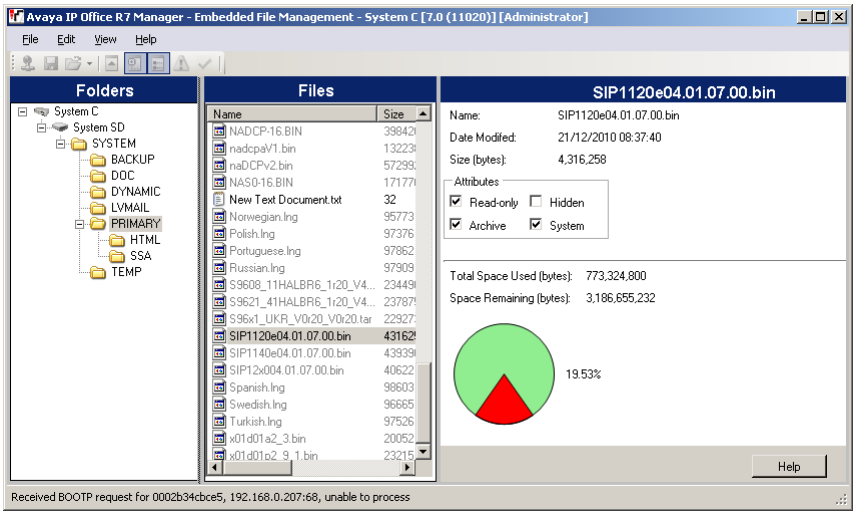
Procedimiento

1. En IP Office Manager, seleccione **Archivo** > **Avanzada** > **Administración de archivos integrada**.

   Se muestra el menú de **Seleccionar IP Office**.

2. Seleccione el sistema telefónico y haga clic en **Aceptar**.
3. Introduzca el nombre y la contraseña del sistema.

   Aparecerá el contenido de la tarjeta de memoria.



4. Siga una de estas opciones:
   - Para IP500 V2, vaya a **SD del sistema** > **SISTEMA** > **PRIMARIO**.
   - Para IP Office Server Edition, vaya a **SISTEMA** > **PRIMARIO**.
5. Para copiar los archivos, realice cualquiera de las siguientes acciones:
   - Arrástrelos desde **PRIMARIO** y suéltelos en la tarjeta de memoria.
   - Vaya a **Archivo** > **Cargar archivos de sistema** > **Carga de archivos de teléfonos** y seleccione el archivo que desea copiar.

   Los archivos de origen se pueden encontrar en la PC de IP Office Manager en `C:\Program Files\Avaya\IPOffice\Manager\memory Cards\Common \system\primary.`.

Vínculos relacionados

[Configuraciones del servidor de archivos](#) en la página 46

Copia manual de los archivos

Acerca de esta tarea

Los archivos se pueden copiar a la tarjeta de memoria colocándola en una PC con una ranura adecuada para tarjetas de memoria.

⚠ Advertencia:

- La tarjeta de memoria no se debe quitar nunca de un sistema en ejecución sin apagarlo primero mediante el siguiente proceso.

Procedimiento

1. Con IP Office Manager, seleccione **Archivo** > **Avanzada** > **Comando tarjeta de memoria** > **Desconectar**.

   Se muestra el menú **Seleccionar IP Office**.
2. Seleccione el sistema telefónico y haga clic en **Aceptar**.
3. Introduzca el nombre y la contraseña del sistema.
4. Puede que se le consulte qué tarjeta desea apagar. Seleccione **SISTEMA** y haga clic en **Aceptar**.
5. En la parte posterior de la unidad de control, verifique que el LED de la ranura de la tarjeta de memoria esté apagado antes de sacar la tarjeta de memoria.
6. Coloque la tarjeta en la ranura para tarjetas de memoria de la PC y examine el contenido.
7. En el sistema IP500 V2, vaya a **SD del sistema** > **SISTEMA** > **PRIMARIO**.

   Los archivos de origen se pueden encontrar en la PC de IP Office Manager en `C:\Program Files\Avaya\IP Office\Manager\memory Cards\Common \system\primary`.

Resultado

Cuando se vuelve a insertar la tarjeta en el sistema, el uso de la tarjeta se reinicia automáticamente.

Vínculos relacionados

Configuraciones del servidor de archivos en la página 46

Carga de archivos en un servidor de terceros

Los archivos de firmware del teléfono se instalan como parte de la aplicación IP Office Manager y se encuentran en el directorio de instalación de la aplicación. De manera predeterminada, el directorio se encuentra en `c:\Program Files\Avaya\IP Office \Manager`.

También pueden obtenerse directamente los mismos archivos de firmware desde el paquete de software que se utiliza para instalar IP Office Manager sin tener que llevar a cabo la instalación. Los archivos se encuentran en la subcarpeta `\program files\Avaya \IPOffice\Manager` del directorio de instalación.

Tenga en cuenta que estos conjuntos de archivos incluyen los archivos .bin que también se emplean para otros dispositivos, incluido el sistemaIP Office mismo.

Vínculos relacionados

Configuraciones del servidor de archivos en la página 46

Capítulo 7: Creación de usuarios y extensiones

Cuando un nuevo teléfono H.323 se registra en el sistema, el sistema puede crear automáticamente una nueva entrada de extensión para el teléfono de su configuración. También puede crear automáticamente una nueva entrada de usuario para el teléfono. En forma alternativa, el teléfono se registra usando un número de extensión para el cual ya existen entradas, y dichas entradas se usan siempre que ningún otro teléfono las esté empleando.

Para nuevas instalaciones, Creación automática puede utilizarse para facilitar el agregado de múltiples teléfonos. Las opciones de creación automática pueden deshabilitarse después de la instalación. Si no se utiliza la Creación automática, las entradas de extensiones y usuarios tienen que agregarse manualmente a la configuración antes de intentar instalar los teléfonos.

Vínculos relacionados

Contraseña de la extensión predeterminada en la página 54
Creación manual de usuarios en la página 55
Crear manualmente las extensiones en la página 55
Selección del códec requerido en la página 56
Uso de la función de creación automática en la página 57

Contraseña de la extensión predeterminada

Acerca de esta tarea

El registro de la mayoría de los teléfonos SIP requiere ingresar una contraseña. Esto puede configurarse a través de la configuración de **Contraseña predeterminada de extensión** del sistema. De manera alternativa, para una extensión en particular, se puede configurar una contraseña específica a través de la configuración de extensiones.

La configuración de extensiones creadas automáticamente en un sistema no puede habilitarse hasta que se configure este valor. Luego, se utiliza como la contraseña para cualquier extensión creada automáticamente.

Procedimiento

1. Con IP Office Manager o IP Office Web Manager en modo sin conexión, cargue la configuración del sistema.
2. Seleccione **SISTEMA** o **Configuración del sistema** > **SISTEMA**.
3. Seleccione **VoIP**.
4. Seleccione **Seguridad VoIP**.

5. En la sección **Contraseña predeterminada de extensión**:
   a. Haga clic en el icono para ver/ocultar la contraseña actual.
   b. Si fuera necesario, cambie o elimine la contraseña.

      La contraseña puede estar en blanco o tener una longitud de 9 a 13 dígitos (0-9).
6. Guarde la configuración.

Vínculos relacionados

Creación de usuarios y extensiones en la página 54

Creación manual de usuarios

Acerca de esta tarea

Si la opción Creación automática de usuario no está activada, debe crear manualmente un usuario para cada teléfono que se va a instalar. Use el procedimiento a continuación para crear manualmente una entrada. También indicará si también debe crearse una entrada de extensión coincidente.

Procedimiento

1. Utilizando IP Office Manager, recupere la configuración del sistema.
2. Para mostrar la lista de usuarios existentes, haga clic en **Usuario**.
3. Haga clic con el botón derecho en el panel derecho y seleccione **Nuevo**.
   a. En la ficha **Usuario**, defina lo siguiente:
      - **Nombre**: ingrese un nombre para el usuario de la extensión. El nombre debe ser único. Si el correo de voz está activo, este nombre se utiliza como la base para un nuevo buzón con el mismo nombre.
      - **Extensión**: esta debe coincidir con el número de extensión.
   b. Haga clic en **Aceptar**.

      IP Office Manager le solicita que cree una extensión que coincida.
   c. Seleccione **Extensión H.323** e introduzca la contraseña del teléfono correspondiente a la extensión, y haga clic en **Aceptar**.
4. Guarde la configuración.

Vínculos relacionados

Creación de usuarios y extensiones en la página 54

Crear manualmente las extensiones

Acerca de esta tarea

Si la opción Creación automática de ext. no está activada, debe crear manualmente una entrada de extensión para cada teléfono que se va a instalar. Esto puede hacerse como parte

del proceso de creación manual de usuarios o debe hacerse por separado usando los procesos a continuación.

Procedimiento

1. Utilizando IP Office Manager, recupere la configuración del sistema.
2. Para mostrar la lista de extensiones existentes, haga clic en **Extensión**.
3. Haga clic en **Nuevo**.
4. En la ficha **Extn**, defina lo siguiente:
   a. **Id. de extensión**: para una extensión VoIP, ingrese un número único, es decir, que no esté siendo utilizado por otra extensión.
   b. **Extensión de base**: ingrese el número de extensión que desea asignar al teléfono. Este número también debe ser único. Este valor se usa para asociar la extensión con el usuario que tiene el mismo número de extensión.
   c. **Contraseña del teléfono**: esta es la contraseña que se utiliza para registrar el teléfono en el sistema. Si no se configura, se utiliza el **Código de inicio de sesión** del usuario que coincida.
5. Para agregar la nueva extensión, haga clic en **Aceptar**.
6. Guarde la configuración.

Vínculos relacionados

Creación de usuarios y extensiones en la página 54

Selección del códec requerido

Acerca de esta tarea

Si **Selección de códec** está configurado en **Predeterminado del sistema**, la extensión utiliza las preferencias de códec del sistema. En la mayoría de los casos, se prefiere esta configuración y cualquier cambio se debe realizar a nivel de sistema para asegurar la consistencia para todas las líneas troncales y las extensiones IP.

Sin embargo, si es necesario, es posible ajustar la **Selección de códec** de cada línea troncal y extensión individual para que sea diferente a los valores predeterminados del sistema.

Procedimiento

1. Utilizando IP Office Manager, recupere la configuración del sistema.
2. Para mostrar la configuración de la extensión, haga clic en **Extensión**.
3. Seleccione la ficha **VoIP**.
4. Cambie el **Selección de códec** a **Personalizar**.

   Las listas **Sin usar** y **Seleccionados** pueden usarse para seleccionar los códecs que usa el dispositivo y su orden de preferencia.
5. Guarde la configuración.

Vínculos relacionados

Creación de usuarios y extensiones en la página 54

Uso de la función de creación automática

Acerca de esta tarea

Cuando instala una gran cantidad de teléfonos, a menos que la configuración se haya creado previamente, puede usarse la creación automática para simplificar el proceso de instalación. Los usuarios creados automáticamente también se vinculan de manera automática a la configuración de derechos del usuario de Creación automática de IP. De manera predeterminada, las llamadas salientes están anuladas en ese conjunto de derechos del usuario.

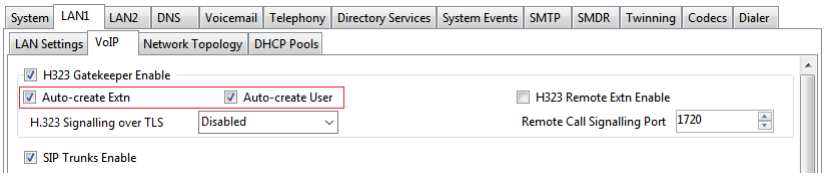
- Deshabilitación automática de creación automática: se recomienda encarecidamente no dejar habilitadas la extensión de creación automática y la configuración del usuario. Para la versión 9.1 y superior, el sistema deshabilita automáticamente la configuración 24 horas después de su habilitación.
- No compatible con licencias WebLM: las opciones de creación automática de extensiones y usuarios no pueden utilizarse en sistemas configurados para adquirir licencias a través de un servicio WebLM.

Antes de empezar

Para sistemas con versión R11.0.4.0 y superiores, configure la Contraseña de extensión predeterminada antes de habilitar la creación automática.

Procedimiento

1. Utilizando IP Office Manager, recupere la configuración del sistema.
2. Seleccione **SISTEMA**.
3. Seleccione la ficha **LAN1** o **LAN2** según la interfaz LAN del sistema que desee usar para admitir las extensiones H.323.
4. Seleccione la subficha **VoIP**.



5. Establecer la configuración de **Creación automática de extensión** y **Creación automática de usuario**.

   Nota:

   Es necesario crear manualmente las entradas de extensiones y/o crear manualmente las entradas de usuarios antes de instalar los teléfonos.

   En sistemas anteriores a la versión 11.0.4.0, cuando se selecciona **Creación automática de extensión**, establezca y confirme una contraseña. La contraseña se establece como Contraseña del teléfono para cualquier extensión creada mediante creación automática. La contraseña del teléfono se usa para el registro.
6. Guarde la configuración.

Vínculos relacionados

Creación de usuarios y extensiones en la página 54

Capítulo 8: Conexión del teléfono

Acerca de esta tarea

En este proceso el teléfono se conecta a la fuente de energía y la red LAN Ethernet. En cuanto el teléfono esté encendido, comenzará a solicitar información.

Antes de empezar

Asegúrese de haber completado la instalación del teléfono antes de comenzar a conectarlo.

Procedimiento

1. Conecte el cable LAN de red a la toma de ingreso de datos de la fuente de alimentación utilizada por el teléfono.
2. Conecte el cable LAN suministrado con el teléfono IP desde la toma de salida de potencia y datos de la fuente de alimentación a la toma que tiene el símbolo de un puerto LAN en la parte trasera del teléfono IP.

   El indicador de mensajes del teléfono debe encenderse de color rojo durante unos segundos. El teléfono comienza el proceso de carga de software. Después de una breve demora, el teléfono muestra `Inicializando` y luego `Cargando`. La fase de carga puede demorar unos minutos.

   - Si el teléfono tiene un archivo de inicio de software existente (es decir, que se instaló anteriormente), carga ese archivo y luego muestra el mensaje `Iniciando`.
3. Si el teléfono muestra el mensaje `No Ethernet (Sin Ethernet)`, verifique la conexión hacia la red LAN.

   El teléfono mostrará `DHCP` y un temporizador cuando intente solicitar una dirección IP y otra información a un servidor DHCP.
4. Presione * mientras aparece `DHCP` para cambiar a la instalación de dirección fija. Consulte Instalación de direcciones fijas.

   Después de unos segundos, la negociación de DHCP finaliza. Si transcurren más de 60 segundos, el temporizador indica la presencia de un error en la configuración de la red o el servidor DHCP.

   Una vez que DHCP se ha completado exitosamente, el teléfono solicitará archivos del servidor de archivos que se indica en la respuesta de DHCP. El primer archivo solicitado detalla los otros archivos que el teléfono también debe cargar. El teléfono hace su solicitud de archivos usando HTTPS. Si esto falla, hace la misma solicitud usando HTTP. Si eso falla, hace una solicitud final usando TFTP. Si todas las solicitudes de un archivo fallan, el teléfono pasa a una alternativa usando la versión actual del archivo que tenga en su propia memoria.

   El teléfono atraviesa un ciclo de solicitud, carga y transferencia de archivos a la memoria Flash.

Después de la carga de archivos, el teléfono muestra `Ext. =`. Vea Registro del teléfono en la página 59.

Vínculos relacionados

Registro del teléfono en la página 59
Elaboración de una lista de teléfonos registrados en la página 60

Registro del teléfono

Acerca de esta tarea

En los teléfonos nuevos y los teléfonos que se hayan reiniciado, el teléfono solicita un número de extensión.

- Si la creación automática está habilitada, el número de extensión utilizado, de estar libre, crea una nueva extensión y entradas de usuario en la configuración de IP Office.
- Si la creación automática no está habilitada, el número de extensión utilizado deberá coincidir con una entrada de extensión VoIP de la configuración de IP Office; consulte Crear manualmente las extensiones en la página 55.

Procedimiento

1. En **Extn**, ingrese el número de extensión que el teléfono debe utilizar y presione #.

   Nota:

   El teléfono muestra `Tipo de equipo incorrecto` si intenta utilizar el número de extensión de una extensión no IP existente.

2. En **Contraseña**, realice una de estas acciones:

   - Si usa la función de creación automática de una extensión, introduzca la contraseña especificada al habilitar la creación automática.
   - Si no se utiliza la creación automática, ingrese **Contraseña del teléfono** según la configuración del sistema para la extensión. Si no se configuró una **Contraseña del teléfono**, el sistema realiza la verificación con el **Código de inicio de sesión** del usuario.

   Nota:

   El sistema deshabilita el uso de contraseñas predeterminadas, como 0000, que algunos teléfonos admiten. Vea Bloqueo de claves predeterminadas en la página 28.

3. Verifique que pueda hacer y recibir llamadas en la extensión.

Vínculos relacionados

Conexión del teléfono en la página 58

Elaboración de una lista de teléfonos registrados

Acerca de esta tarea

La aplicación System Monitor puede usarse para verificar qué teléfonos están registrados en el sistema.

Procedimiento

1. Inicie System Monitor y conéctese al sistema IP Office.
2. Seleccione **Estado** > **Estado del teléfono H.323**.

Resultado

System Monitor muestra los teléfonos registrados y cuántos están esperando para registrarse. Para ver estos mensajes, debe seleccionarse la opción de filtro **SISTEMA** > **Imprimir seguimiento**.

Aparece lo siguiente como líneas similares a:

```
792ms PRN: GRQ de c0a82c15 --- RAS alcanza la capacidad máxima de 10;
41 extremos registrados.
```

Vínculos relacionados

Conexión del teléfono en la página 58

Parte 3: Configuración opcional

Capítulo 9: Activación de supervisión de la calidad de RTCP

Los teléfonos IP de Avaya admiten supervisión de la calidad de la llamada. La activación de la supervisión de RTCP proporciona al sistema mediciones de retraso de paquetes, pérdida de paquetes y fluctuación. Se puede acceder a esa información usando System Status Application y System Monitor. El sistema también puede configurarse para alarmas de salida cuando los valores de calidad de la llamada superan los niveles establecidos.

Los informes de calidad de llamadas de RTCP también pueden enviarse a la dirección de una aplicación de supervisión de QoS de un tercero.

En el caso de la versión 10.0 de IP Office y posteriores, además de que los teléfonos individuales pueden enviar informes de calidad de llamadas RTCP, el sistema también puede enviar informes RTCP para llamadas.

Vínculos relacionados

Habilitación de informes de calidad del teléfono en la página 62
Habilitación de informes de calidad del sistema en la página 63
Configuración de niveles de alarma de calidad en la página 64

Habilitación de informes de calidad del teléfono

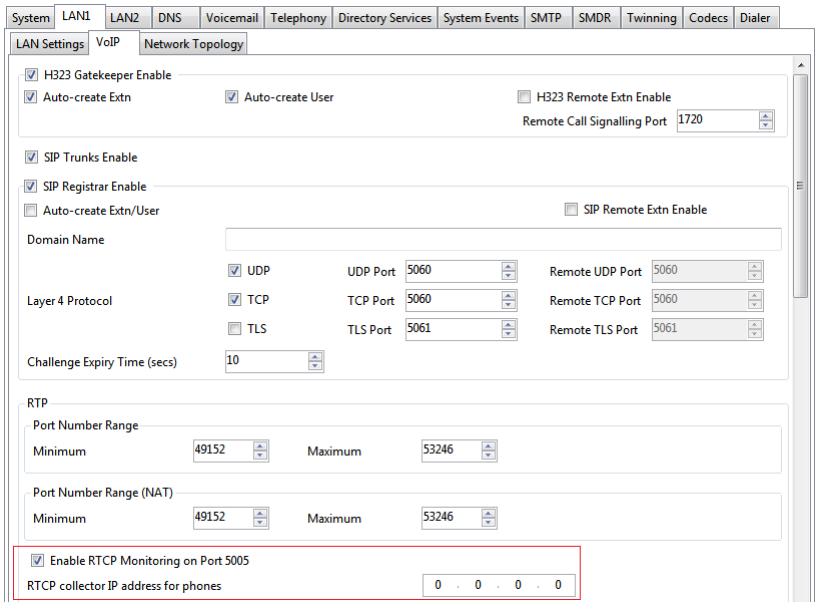
Acerca de esta tarea

La habilitación de los informes de calidad de llamadas de RTCP desde los teléfonos se realiza desde la configuración del sistema.

Procedimiento

1. Utilizando IP Office Manager, recupere la configuración del sistema.
2. Seleccione **SISTEMA**.
3. Seleccione la ficha **LAN1** o **LAN2** según la interfaz LAN del sistema que desee usar para admitir las extensiones H.323.

4. Seleccione la subficha **VoIP**.



5. Habilite la casilla de verificación **Habilitar control RTCP en puerto 5005**.

   De manera predeterminada, los datos de RTCP se envían al sistema IP Office. Ingrese la dirección en el campo **Dirección IP del recopilador RTCP para teléfonos** para teléfonos y envíe datos a una dirección específica para que la recopile una aplicación de control de calidad de servicio de terceros.

6. Guarde la configuración.

Vínculos relacionados

Activación de supervisión de la calidad de RTCP en la página 62

Habilitación de informes de calidad del sistema

Acerca de esta tarea

En el caso de la versión 10.0 de IP Office y posteriores, además de que los teléfonos individuales pueden enviar informes de calidad de llamadas RTCP, el sistema también puede enviar informes RTCP para llamadas.

Procedimiento

1. Utilizando IP Office Manager, recupere la configuración del sistema.
2. Seleccione **SISTEMA**.
3. Seleccione la ficha **Telefonía** y luego la subficha **Telefonía**.
4. Vaya a la sección **Configuración de recopilador RTCP**.
   a. Habilite la casilla de verificación **Enviar RTCP a un recopilador RTCP**.
   b. En **Dirección del servidor**, agrega la dirección de la aplicación de Control de servicio de calidad de terceros a la que el sistema envía los informes RTCP.

c. En **Número de puerto UDP**, ingrese el puerto de destino. El valor predeterminado es 5005.

d. En **Intervalo de informes RTCP**, ingrese con qué frecuencia el sistema envía informes RTCP.

5. Guarde la configuración.

Vínculos relacionados

Activación de supervisión de la calidad de RTCP en la página 62

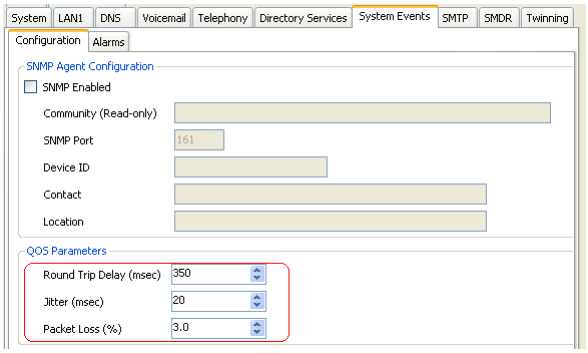
Configuración de niveles de alarma de calidad

Acerca de esta tarea

El sistema puede enviar alarmas de calidad de llamada a System Status Application. También puede enviar las mismas alarmas a SNMP, correos electrónicos o destinos Syslog. Para obtener detalles sobre cómo configurarlas, consulte la documentación de IP Office Manager. La siguiente configuración se usa para establecer los niveles que, de superarse, hacen que se envíe una alarma al final de una llamada.

Procedimiento

1. Utilizando IP Office Manager, recupere la configuración del sistema.
2. Seleccione **SISTEMA**.
3. Seleccione la ficha **Eventos del sistema** y luego la subficha **Configuración**.



Los parámetros de QoS los emplea el sistema para generar alarmas La configuración predeterminada coincide con los límites generalmente aceptables para una llamada de buena calidad.

4. Guarde la configuración.

Vínculos relacionados

Activación de supervisión de la calidad de RTCP en la página 62

Capítulo 10: Protector de pantalla

Después de un período de inactividad configurado, los teléfonos de la serie 9600 pueden mostrar una imagen de protector de pantalla. Mientras el teléfono está inactivo, esta imagen se mueve a otra posición aleatoria en la pantalla cada cinco (5) segundos.

En el caso de los teléfonos completamente compatibles con el sistema IP Office, el sistema IP Office proporciona automáticamente un archivo predeterminado. De lo contrario:

- El tiempo de espera del protector de pantalla y el nombre del archivo de imagen se establecen mediante la personalización del archivo `46xxsettings.txt`.
- El archivo de imagen que se utilizará debe cargarse en el servidor de archivos que usan los teléfonos.

Estos son los requerimientos de imagen:

- Formato: imágenes JPG.
- Tamaño máximo de píxel: la imagen debe ser inferior al tamaño de la pantalla del teléfono. Si la imagen es más grande, no se mostrará. Cuando hay varios tipos de teléfonos con la misma imagen, esta debe ser inferior al tamaño máximo de todos los tipos de teléfonos. Si se utiliza el archivo 46xxsettings.txt para especificar la configuración del protector de pantalla, es posible especificar una imagen por separado para cada tipo de teléfono.

Teléfono	Tamaño máximo
9611	160X160
9621G	320X160
9614G	320X240

- Pantallas a color: la profundidad del color es de 16 bits. Una imagen a color por separado presenta la mejor apariencia.
- Pantallas monocromáticas: Logrará mejores resultados con una imagen de logotipo con una sola escala de grises. También admite dos niveles de escala de grises.
- Transparencia: para invocar un fondo transparente, utilice un color de fondo de 0,255,0 (el verde más brillante posible).

La configuración predeterminada de IP Office usa un archivo de imagen denominado 96xxiposs.jpg. Con el administrador de archivos integrado en IP Office Manager, reemplace el archivo existente en la carpeta /primary del sistema con su imagen personalizada. Reinicie los teléfonos para que carguen la imagen nueva.

Vínculos relacionados

Personalización de la configuración del protector de pantalla en la página 66

Personalización de la configuración del protector de pantalla

Acerca de esta tarea

El funcionamiento predeterminado utiliza la imagen `96xxiposs.jpg` que usted puede reemplazar con su propia imagen. Si usa un archivo `46xxsettings.txt` personalizado, puede implementar el tiempo de espera en inactividad para que se muestre el protector de pantalla y el nombre de la imagen.

Procedimiento

1. Cree un archivo JPG del cliente cumpliendo con los requisitos.

   Para este ejemplo utilizamos el nombre de archivo `logo.jpg`.

2. Descargue el archivo `46xxsettings.txt` actual del servidor de archivos que usan los teléfonos.

3. Agregue las siguientes líneas al archivo `46xxsettings.txt`:

   ```
   Nombre de archivo ## SET SCREENSAVER
   SET SCREENSAVER logo.jpg
   ## SET SCREENSAVERON tiempo en minutos antes de la activación
   SET SCREENSAVERON 40
   ```

   - Con imágenes separadas para cada tipo de teléfono

     La adición de lo anterior al inicio del archivo afecta a todo tipo de teléfono. La adición de distintas configuraciones a cada una de las distintas secciones de MODEL4 del archivo para cada tipo de teléfono permite usar imágenes separadas para cada tipo de teléfono.

4. Cargue los nuevos archivos al servidor de archivos que usan los teléfonos.

5. Reinicie los teléfonos para que carguen la imagen y la configuración nuevas.

Vínculos relacionados

Protector de pantalla en la página 65

Capítulo 11: configuraciones de copia de seguridad/restauración

Los teléfonos IP H.323 de la serie 1600 y 9600 admiten el uso de un servidor HTTP como la ubicación en la cual se realizan copias de seguridad y se restauran los datos específicos del usuario. La dirección para este servidor de copia de seguridad se configura de forma separada a la del servidor de archivos que se utiliza para firmware del teléfono.

Estas opciones se utilizan si se ha especificado la ubicación del servidor HTTP para la copia de respaldo/restauración en el `46xxsettings.txt` archivo del teléfono.

- La dirección del servidor HTTP para la operación de copia de seguridad/restauración es independiente de la dirección del servidor HTTP utilizada para las descargas de archivos de firmware del teléfono.
- El servidor HTTP que se utiliza para la copia de seguridad/restauración requerirá cambios de configuración para permitir que los teléfonos le envíen archivos.
- Si el sistema IP Office se utiliza como servidor de archivos para la instalación del teléfono, también puede utilizarse para las funciones de copia de seguridad y restauración del teléfono. Eso incluye la generación automática de archivos. Cuando se utiliza la generación automática, algunos valores de configuración contenidos dentro del archivo de restauración se basan en la configuración de IP Office del usuario. Por lo tanto, esta es la solución recomendada cuando sea posible.

La copia de seguridad se utiliza cuando el usuario del teléfono cierra sesión en el teléfono. Durante el proceso de cierre de sesión, el teléfono crea un archivo que contiene los datos específicos del usuario y los envía a la ubicación del valor BRURI. El nombre del archivo se compone del número de extensión del usuario como prefijo de `_16xxdata.txt`; por ejemplo, `299_16xxdata.txt`.

La restauración se utiliza cuando un usuario inicia sesión en ese teléfono. El teléfono envía una solicitud del archivo apropiado según el número de extensión del usuario. Si el archivo se recupera con éxito, el teléfono importará la configuración y, después de que aparezca el mensaje `"La recuperación se realizó correctamente"`, continuará funcionando normalmente. Si el archivo no puede recuperarse, aparecerá el mensaje `"No se pudo realizar la recuperación"` y el teléfono continuará con la configuración existente.

Vínculos relacionados

Especificación del valor BRURI en la página 68
Autenticación de HTTP en la página 68
Control de copia de seguridad/ restauración manual en la página 69
Archivo de ejemplo en la página 69

Especificación del valor BRURI

Acerca de esta tarea

Si está usando el sistema IP Office como el servidor de archivos, se recomienda que también lo use como el servidor de copia de seguridad y restauración. Para esta opción no se requiere configuración adicional. Si no hay archivo `46xxsettings.txt` en el sistema IP Office, generará automáticamente el archivo cuando un teléfono lo solicite e incluirá su propia dirección IP como la dirección del servidor de copia de seguridad/restauración. Si hay un archivo `46xxsettings.txt` en el sistema IP Office, puede editar manualmente la dirección del servidor de copia de seguridad/restauración usando el proceso a continuación para que concuerde con la dirección IP del sistema.

Si desea usar otro servidor, edite el valor `BRURI` en el archivo `46xxsettings.txt`. También necesitará asegurar que el servidor que se va a usar esté configurado para que permita la carga de archivos a la carpeta especificada en el servidor.

Procedimiento

1. Abra el archivo `46xxsettings.txt`.
2. Localice la línea que contiene el valor **CONFIGURAR BRURI**.
3. Si la línea tiene caracteres # como prefijo, elimínelos y también borre los espacios.
4. Después de `SET BRURI`, ingrese un espacio y luego la dirección del servidor de copia de seguridad HTTP:
   - Por ejemplo `SET BRURI http://192.168.0.28`
   - Si es necesario, especifique la ruta a un directorio de servidor específico o incluya un número de puerto específico, por ejemplo: `SET BRURI http://192.168.0.28/backups:8080`.

Vínculos relacionados

configuraciones de copia de seguridad/restauración en la página 67

Autenticación de HTTP

La autenticación de HTTP puede admitirse. Si se configura se utilizará para operaciones de copia de seguridad y restauración. El dominio y las credenciales de autenticación se almacenan en la memoria reprogramable no volátil del teléfono, que no se sobrescribe cuando se descarga un nuevo firmware.

El valor predeterminado del dominio y las credenciales de autenticación es "nulo". Si el servidor HTTP requiere autenticación, se le solicitará al usuario que ingrese nuevas credenciales mediante el teléfono. Si la autenticación tiene éxito, los valores utilizados se almacenarán y se utilizarán para operaciones subsiguientes de copia de seguridad y restauración.

Vínculos relacionados

configuraciones de copia de seguridad/restauración en la página 67

Control de copia de seguridad/ restauración manual

Los usuarios pueden solicitar una copia de seguridad o restauración a través de la característica **Avanzada**Copia de seguridad/restauración de opciones avanzadas como se detalla en la guía del usuario para el modelo de teléfono específico.

Vínculos relacionados

[configuraciones de copia de seguridad/restauración](#) en la página 67

Archivo de ejemplo

A continuación figura un ejemplo de un archivo de copia de seguridad/restauración para un usuario de un teléfono de la serie 1600. Cabe observar que los valores no se escriben a menos se haya cambiado la configuración predeterminada.

Si la copia de seguridad y restauración se hace usando generación automática de archivos, dichos elementos indicados mediante * se controlan a través de los valores almacenados y que suministra la configuración de IP Office del usuario.

Archivo	Campos	Descripción
ABKNAME001=Extn201 ABKNUMBER001=201 ABKNAME002=Extn201ad ABKNUMBER002=201 ABKNAME003=Extn203 ABKNUMBER003=203 Redial (Volver a marcar)=0 Call Timer (cronómetro de llamada)=0 Visual Alerting (Alerta visual)=1 Call Log Active (Registro de llamadas activo)=1 Log Bridged Calls (Llamadas de puente del registro)=1 Log Line Calls (Llamadas de línea del registro)=1 Log Calls Answered by Others (Llamadas del registro respondidas por otros)=0 Audio Path (Ruta de audio)=2 Personalized Ring (Timbre personalizado)=7 Handset AGC (AGC del auricular)=1 Headset AGC (AGC del auricular manos libres)=1 Speaker AGC (AGC del altavoz)=1 Error Tone (Tono de error)=1 Button Clicks (Clics de botones)=0	ABKNAMEmmm ABKNUMBERmmm	Estas entradas combinadas se utilizan para los contactos personales ingresados en el teléfono. El valor mmm de cada par es reemplazado por un número de 3 dígitos que comienza con 001. La primera línea del par almacena el nombre de contacto y la segunda línea el número de teléfono del contacto.*
	LANGUSER	Idioma de pantalla. Se almacena el nombre del idioma.*
	LOGACTIVE	Registro de llamadas activo activado (1) o desactivado (0).*
	LOGBRIDGED	Llamadas de puente del registro activado (1) o desactivado (0).*
	LOGLINEAPPS	Llamadas de línea del registro activado (1) o desactivado (0).*
	LOGOTHERANS	Llamadas del registro respondidas por otros activado (1) o desactivado (0).*
	OPTAGCHAND	Handset Automatic Gain Control (Control de ganancia automático del auricular) activado (1) o desactivado (0).

La tabla continúa…

Archivo	Campos	Descripción
Display Language (Mostrar idioma)=English (Inglés)	OPTAGCHEAD	Headset Automatic Gain Control (Control de ganancia automático del auricular manos libres) activado (1) o desactivado (0).
	OPTAGCSPKR	Speaker Automatic Gain Control (Control de ganancia automático del altavoz) activado (1) o desactivado (0).
	OPTAUDIOPATH	Ruta de audio.*
	OPTCLICKS	Button Clicks (Clics de botones) activado (1) o desactivado (0).*
	OPTERRORTONE	Tono de error activado (1) o desactivado (0).*
	PERSONALRING	Personalized Ring (Timbre personalizado). Se almacena un valor numérico (1 a 8) para el timbre seleccionado.*
	PHNREDIAL	Remarcar
	PHNSCRONCALL	Go to call screen on calling (Ir a la pantalla de llamada al llamar) activado (1) o desactivado (0).
	PHNSCRONALERT	Go to call screen on ringing (Ir a la pantalla de llamada al sonar) activado (1) o desactivado (0).
	PHNTIMERS	Cronómetro de llamada activado (1) o desactivado (0). ✓
	PHNVISUALALERT	Alerta visual activado (1) o desactivado (0). ✓

Vínculos relacionados

[configuraciones de copia de seguridad/restauración](#) en la página 67
[Configuración del servidor IIS](#) en la página 70
[Configuración del servidor apache](#) en la página 71

Configuración del servidor IIS

Acerca de esta tarea

Cree una carpeta de copia de seguridad en el directorio de raíz del servidor Web. Todos los archivos de copia de seguridad se almacenarán en ese directorio. Por ejemplo, si su carpeta de copia de seguridad es `C:/Inetpub/wwwroot/backup`, el archivo `46xxsettings.txt` debe tener una línea similar a `SET BRURI http://www.example.com/backup`.

Procedimiento

1. Vaya a **Comenzar** > **Configuración** > **Panel de control** > **Herramientas administrativas** y seleccione, según la versión de Windows, **Administrador de Servicios de Información de Internet (IIS)** o **Servicios de Información de Internet (IIS)**.
2. Haga clic con el botón secundario en la carpeta creada para copia de seguridad. Haga clic con el botón secundario en **Sitio web predeterminado** si no hay un directorio de copia de seguridad específico.
3. Seleccione **Propiedades**.
4. En la ficha **Directorio**, active la casilla de verificación **Escribir**.
5. Siga este procedimiento para configurar IIS 6.0:
   a. Vaya a **Comenzar** > **Configuración** > **Panel de control** > **Herramientas administrativas**.
   b. Debajo de **Sitio web predeterminado**, seleccione **Extensión de servicios web**.
   c. Asegúrese de que la opción **WebDAV** esté configurada en **Permitido**.

Vínculos relacionados

Archivo de ejemplo en la página 69

Configuración del servidor apache

Acerca de esta tarea

Cree una carpeta de copia de seguridad en el directorio de raíz del servidor Web. Debe configurar la carpeta para que todos los usuarios puedan grabar en ella. Todos los archivos de copia de seguridad se almacenarán en ese directorio. Por ejemplo, si la carpeta de copia de seguridad es `C:/Program Files/ApacheGroup/Apache2/htdocs/backup`, el archivo `46xxsettings.txt` debe tener una línea similar a `SET BRURI http://www.example.com/backup`.

Antes de empezar

Procedimiento

1. Edite el archivo de configuración del servidor Web `httpd.conf`.
2. Elimine el comentario de las dos líneas de `LoadModule` relacionadas con DAV:
   - `LoadModule dav_module modules/mod_dav.so`
   - `LoadModule dav_fs_module modules/mod_dav_fs.so`

   Nota:

   Si estos módulos no están disponibles en el sistema (normalmente en algunos servidores Unix/Linux Apache) deberá recopilar estos dos módulos (mod_dav y mod_dav_fs) en el servidor. Es posible que existan otras formas de cargar los módulos. Consulte su documentación de Apache en http://httpd.apache.org/docs/ para obtener más detalles.

3. Agregue las siguientes líneas en el archivo `httpd.conf`:

```
#
Configuración de #WebDAV
#D
avLockDB "C:/Program Files/Apache Group/Apache2/var/DAVLock"
<Location />
Dav activado
</Location>
```

Nota:

Para servidores Web Unix/Linux, la cuarta línea puede ser similar a la siguiente: DavLockDB/usr/local/apache2/var/DAVLock

4. Cree un directorio var y configúrelo para que todos los usuarios puedan grabar en él. Haga clic con el botón secundario en **Propiedades** y seleccione **Seguridad** > **Agregar** > **Todos** > **Control total** > **.**

Vínculos relacionados

Archivo de ejemplo en la página 69

Parte 4: Procesos de instalación avanzados

Capítulo 12: Instalación de direcciones fijas

La instalación de direcciones fijas sólo es necesaria cuando un servidor DHCP no está disponible o no se requiere. Para facilitar el mantenimiento y la instalación, asegúrese de que se utilice un servidor DHCP y evite el direccionamiento fijo. Luego de una actualización de archivo de inicio del firmware del teléfono, puede que se requiera reinstalar la información de dirección fija.

Vínculos relacionados

Instalación de dirección fija para teléfonos de la serie 1600 en la página 74
Configuración de instalación de dirección fija para la serie de teléfonos 1600 en la página 75
Instalación de dirección fija para teléfonos de la serie 9600 en la página 75
Configuración de instalación de dirección fija para la serie de teléfonos 9600 en la página 76

Instalación de dirección fija para teléfonos de la serie 1600

Procedimiento

1. Complete el procedimiento de conexión del teléfono y, cuando se muestre `DHCP`, presione * para cambiar el teléfono a la instalación de direcciones fijas.

   El teléfono muestra la secuencia de ajustes y el valor existente para cada uno de esos ajustes.

2. Para aceptar los valores existentes, presione # o ingrese un valor y luego presione #. Vea Configuración de instalación de dirección fija para la serie de teléfonos 1600 en la página 75.

   Nota:

   Si no se cambian valores, el teléfono muestra `Sin valores nuevos`.

3. Si el teléfono muestra `Enter`, apague el teléfono y vuelva a encenderlo.

   Una vez que se ingresan todos los valores o se aceptan los valores existentes, el teléfono muestra `¿Desea guardar los valores nuevos?`.

4. Presione # para guardar los valores.

Pasos siguientes

Registre el teléfono.

Vínculos relacionados

Instalación de direcciones fijas en la página 74

Configuración de instalación de dirección fija para la serie de teléfonos 1600

Nombre de configuración	Descripción
Teléfono	Es la dirección IP del teléfono. Para aceptar el valor actual, presione # o ingrese un valor y luego presione #. Si ingresa un valor nuevo, presione la tecla * para ingresar un carácter "." entre los dígitos.
CallSv	Es la dirección de gatekeeper de H.323. Para sistemas IP Office, esta es la dirección IP de la LAN de IP Office.
CallSvPort	Es el número de puerto del nivel de transporte de Gatekeeper. Para los teléfonos IP de Avaya, el valor que se debe utilizar es 1719. Para aceptar el valor actual, presione # o ingrese un valor y luego presione #.
Enrutador	Es la dirección IP de Gateway predeterminada del teléfono. Para IP Office, normalmente es la dirección IP de LAN de IP Office. Para aceptar el valor actual, presione # o ingrese un valor y luego presione #.
Máscara	Es la máscara IP del teléfono (también conocida como la máscara de subred). La máscara se utiliza con la dirección IP para indicar la subred del teléfono. Debe coincidir con la máscara IP de la unidad de IP Office.
Servidor de archivos	Es la dirección del servidor de archivos al que el teléfono debe solicitar software y archivos de configuración. Ingrese la dirección de TFTP o HTTP que se haya configurado con el archivo de software del teléfono IP de Avaya definido.
802.1Q	Para cambiar la configuración, presione *. Presione # para aceptar el valor.
ID VLAN	Para obtener información sobre la configuración de VLAN, consulte Teléfonos IP y VLAN.

Vínculos relacionados

Instalación de direcciones fijas en la página 74

Instalación de dirección fija para teléfonos de la serie 9600

Procedimiento

1. Cuando aparezca `* para programar`, presione la tecla *.
2. Cuando aparece `Ingrese código`, ingrese el código de acceso de procedimientos administrativos y presione #. El código de acceso predeterminado es CRAFT (27238).
3. Desplácese por el menú hasta ADDR y seleccione esta opción para iniciar el procedimiento direcciones.

Aparecerá la lista de direcciones necesarias. Si se muestra algún valor de teléfono existente. De lo contrario, si el teléfono es nuevo o se ha eliminado, todas las direcciones se configuran en 0.0.0.0.

4. Configure cada dirección, resalte el valor que desea cambiar, y haga clic en **Cambiar**. Consulte la configuración de instalación de direcciones fijas.
5. Ingrese el valor de la nueva dirección y luego seleccione **Guardar**.
6. Cuando todos los valores estén configurados según se necesita, haga clic en **Volver** y haga clic en **Salir**.

   El teléfono se reinicia usando los nuevos valores.

Pasos siguientes

Registre el teléfono.

Vínculos relacionados

Instalación de direcciones fijas en la página 74

Configuración de instalación de dirección fija para la serie de teléfonos 9600

Nombre de configuración	Descripción
Teléfono	Es la dirección IP del teléfono. Para aceptar el valor actual, presione # o ingrese un valor y luego presione #. Si ingresa un valor nuevo, presione la tecla * para ingresar un carácter "." entre los dígitos.
Servidor de llamadas	Es la dirección de gatekeeper de H.323. Para sistemas IP Office, esta es la dirección IP de la LAN de IP Office.
Enrutador	Es la dirección IP de Gateway predeterminada del teléfono. Para IP Office, normalmente es la dirección IP de LAN de IP Office. Para aceptar el valor actual, presione # o ingrese un valor y luego presione #.
Máscara	Es la máscara IP del teléfono (también conocida como la máscara de subred). La máscara se utiliza con la dirección IP para indicar la subred del teléfono. Debe coincidir con la máscara IP de la unidad de IP Office.
Servidor de archivos HTTP	Es la dirección del servidor de archivos HTTP al que el teléfono debe solicitar software y archivos de configuración.
Serv arch HTTPS	Es la dirección del servidor de archivos HTTPS al que el teléfono debe solicitar software y archivos de configuración. El teléfono intentará usar esta dirección, si está configurada, antes de utilizar HTTP.
802.1Q	Para cambiar la configuración, presione *. Presione # para aceptar el valor.
ID VLAN	Para obtener información sobre la configuración de VLAN, consulte Teléfonos IP y VLAN.
Prueba VLAN	Al usar VLAN, este el tiempo en segundos que el teléfono esperará por una respuesta del servidor DHCP en la VLAN antes de pasar a operación sin VLAN normal.

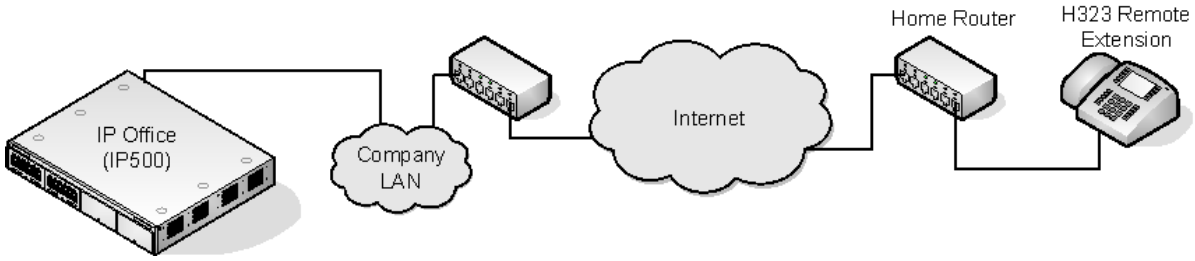
Vínculos relacionados

Instalación de direcciones fijas en la página 74

Capítulo 13: Extensiones remotas de H.323

Para la versión 8.0 de IP Office, la configuración de extensiones H.323 remotas es compatible sin ser necesario que esas extensiones utilicen firmware VPN especial. Esta opción está diseñada para ser utilizada en la siguiente situación:

- El cliente LAN posee una dirección IP pública la cual es remitida al sistema IP Office. Esta dirección es utilizada como la dirección del servidor de llamada por las extensiones H.323 remotas.
- El usuario posee un teléfono H.323 en un enrutador doméstico. Se supone que el enrutador doméstico permite que todo el tráfico saliente desde la red pase y permite todo el tráfico simétrico. Es decir, si el teléfono envía RTP/RTCP a una dirección IP y puerto público, podrá recibir RTP/RTCP desde la misma dirección IP y puerto público. En esta configuración no se tratan otras configuraciones.



- El sistema puede configurarse para admitir extensiones H.323 remotas cuando se utiliza NAT en la ruta de conexión. Esto podría suceder cuando IP Office está ubicado detrás de un enrutador NAT/Firewall corporativo y/o el teléfono H.323 está ubicado detrás de un enrutador residencial activador de NAT. El uso de esta opción y la interacción y configuración de elementos ajenos externos está fuera del alcance de este archivo de ayuda.
- Cuando se desconoce la dirección IP pública del enrutador corporativo, debe configurar un servidor STUN en la configuración 'Topología de red de la red LAN de IP Office. Tenga en cuenta que aunque esta opción no sea compatible si el Tipo de firewall/NAT está configurado en Firewall simétrico o Abrir Internet.
- Habilitar la opción Permitir extn remota también muestra la configuración de ajustes del Rango de números de puerto (NAT) de RTP.
- Teléfonos compatibles: actualmente, la operación de extensiones H.323 remotas sólo es compatible con los teléfonos de la Serie 9600 compatible con el sistema IP Office.
- Requisitos de licencia: de forma predeterminada, sólo cuatro (4) usuarios pueden configurarse para el uso de extensiones H.323 remotas sin licencia. Se pueden configurar usuarios adicionales si estos usuarios poseen una licencia y son configurados ya sea mediante perfiles de usuario de **Teleworker** o **Power User**.

Vínculos relacionados

Configuración de red de cliente en la página 79
Configuración del sistema IP Office en la página 80
Configuración de teléfono en la página 81

Configuración de red de cliente

El alojamiento LAN corporativo del sistema IP Office requiere de una dirección IP pública enrutada a la interfaz LAN del sistema IP Office configurado para admitir las extensiones H.323 remotas.

STUN desde el sistema IP Office a la Internet se utiliza para determinar el tipo de NAT aplicado al tráfico entre el sistema e Internet. Cualquier dispositivo enrutador o firewall existente entre la ubicación del teléfono H.323 y el sistema IP Office debe permitir el siguiente tráfico.

Protocolo	Puerto	Descripción
ICMP	-	Se debe permitir ICMP entrante a la dirección IP pública del sistema IP Office.
UDP	1719	Tráfico de Puerto UDP 1719 al sistema IP Office debe ser permitido. Esto se utiliza para procesos RAS H225 tales como descubrimiento de gatekeeper, registro, control, etc. Si este puerto no está abierto, el teléfono no podrá registrarse con el sistema IP Office.
TCP	1720	Tráfico de puerto TCP 1720 debe ser permitido. Esto se utiliza para H.225 (señalización de la llamada). La dirección que se utiliza puede ajustarse con la configuración Puerto de señalización de llamada remota.
RTP	Varios	Se deben permitir los puertos en el rango especificado por la configuración del Rango de números de puerto (NAT) de RTP.
RTCP		
UDP	5005	Si la configuración de sistema Habilitar supervisión de RTCP en puerto 5005 ha sido habilitada, se debe permitir el tráfico en este puerto para incluir las extensiones H.323 remotas en la supervisión.

Configuración de red de usuario

Se supone que el enrutador doméstico permite que todo el tráfico saliente desde la red pase y permite todo el tráfico simétrico. Es decir, si el teléfono envía RTP/RTCP a una dirección IP y puerto público, el enrutador permite que reciba RTP/RTCP desde la misma dirección IP y puerto público.

Vínculos relacionados

Extensiones remotas de H.323 en la página 78

Configuración del sistema IP Office

Acerca de esta tarea

Este es un resumen de los cambios necesarios en la configuración del sistema IP Office. Esta sección asume que ya está familiarizado con la instalación del sistema IP Office y del teléfono IP H.323

Antes de empezar

Si se van a admitir más de 4 usuarios de extensión remota, el sistema debe incluir **Teleworker** disponibles y/o licencias **Power User** para esos usuarios.

Procedimiento

1. En la ficha **SISTEMA**, configure lo siguiente:
   a. Vaya a **SISTEMA** > **LAN1** > **LAN2** > **VoIP**.
   b. Habilite la casilla de verificación **Habilitar Gatekeeper de H323**.

      Nota:

      Debido a las configuraciones adicionales para usuario y extensión para la configuración de extensiones H.323 remotas, la extensión y entradas de usuario para las extensiones H.323 remotas y usuarios son añadidas en forma manual.

   c. Habilite **Habilitar extn remota H.323**.
   d. Ingrese el valor requerido en **Puerto de señalización de llamada remota**.

      El valor predeterminado 1720 también coincide con el puerto utilizado por las extensiones internas.

   e. Configure **Intervalo de números de puerto (NAT) RTP** para abarcar el rango de puertos que debería usarse para el tráfico de RTP y RTCP de extensiones H323.

      Nota:

      La configuración del rango debe proporcionar al menos dos (2) puertos admitidos por extensión.

2. En la ficha **Topología de red**, configure lo siguiente:

   Nota:

   STUN puede ser utilizada para determinar el tipo de procesos firewall/NAT que se aplican al tráfico entre el sistema IP Office e Internet.

   a. Vaya a **Topología de red** y configure **Dirección IP del servidor STUN** a un servidor STUN conocido.
   b. Haga clic en **Aceptar**

      El botón **Ejecutar STUN** está habilitado.

   c. Haga clic en **Ejecutar STUN** y espere un momento a que el proceso STUN se ejecute.

      Los resultados descubiertos por el proceso son indicados por los íconos ! junto a los campos.

d. Si STUN informa que **Tipo de Firewall/NAT** en la que la red debe volver a configurarse.

Nota:

Los tipos de red **Bloqueo de puertos estáticos**, **NAT simétrico** y **Internet abierto** no son compatibles con extensiones H.323 remotas.

3. En la ficha **Usuario**, configure lo siguiente:
   a. Vaya a la ficha **Usuario**, configure el **Perfil de usuario** en **Teleworker** o **Power User**.
   b. Habilite **Habilitar Remote Worker**.

Vínculos relacionados

Extensiones remotas de H.323 en la página 78

Configuración de teléfono

Los teléfonos no requieren ningún firmware especial. Por lo tanto, deben ser instalados primero como extensiones internas normales, durante lo cual se cargará el firmware proporcionado por el sistema IP Office.

Una vez que este proceso haya finalizado, la configuración de dirección del teléfono debe ser borrada y la dirección del servidor de llamada debe ser configurado con la dirección pública que utilizará la extensión H.323 remota.

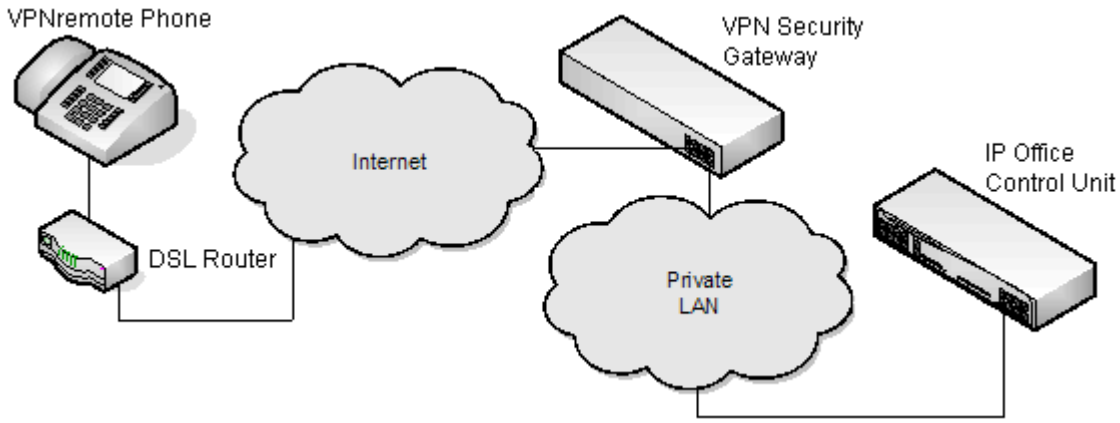
Se supone que en la ubicación remota, el teléfono obtendrá otra información de dirección por DHCP desde el enrutador del usuario. Si este no es el caso, la otra configuración de dirección para el teléfono necesitará ser administrada estadísticamente para hacer coincidir las direcciones adecuadas a la red del usuario.

Vínculos relacionados

Extensiones remotas de H.323 en la página 78

Capítulo 14: Teléfonos VPN Remote

Los teléfonos IP de Avaya en ubicaciones remotas pueden conectarse al sistema IP Office mediante túneles IPSec VPN. Esto es compatible para teléfonos 4610SW, 4621SW, 5610SW y 5621SW. También es compatible con los teléfonos de la serie 9600.



Los componentes adicionales necesarios para teléfonos remotos sobre VPN son:

- Firmware del teléfono IP Office VPNremote: este firmware está incluido en el conjunto de firmware del teléfono IP.
- VPN Security Gateway: el sistema IP Office no admite todas las características de IPSec necesarias para teléfonos VPNremote que usan sus propios túneles IPSec. Por lo tanto, el túnel VPN de los teléfonos remotos debe terminar en un dispositivo gateway VPN alternativo adecuado. El dispositivo debe admitir uno de los siguientes métodos:
  - Gateways Avaya: los dispositivos gateway de seguridad Avaya (SG y VSU) utilizan un protocolo patentado de Avaya denominado
    - Serie CCD SG de Avaya (firmware 4.6 o posterior)
    - Serie VSU de Avaya (firmware 3.2 o posterior)
  - Gateways de terceros: los gateways VPN de terceros con Autenticación extendida IKE (Xauth) y con clave compartida previamente (PSK). Los elementos que se detallan a continuación cuentan con notas de instalación. Esto no implica ninguna recomendación de esos dispositivos por parte de Avaya ni se excluyen otros dispositivos.

    Nota:

    Avaya no puede garantizar la compatibilidad de los dispositivos a través de los dispositivos de terceros.

    - Concentradores Cisco VPN de la serie 300
    - Dispositivos de seguridad Cisco PIX de la serie 500

- Dispositivos Juniper Networks NetScreen Series VPN
- Juniper Networks Secure Services Gateway de la serie 500
- Juniper Networks Integrated Security Gateway (ISG) Series
- Enrutador Kentrox Q2300 VPN
- Enrutador Sonicwall Tz170 VPN
- Enrutador Netgear FVS338 VPN
- Enrutador Netgear FVX538 VPN
- Enrutador Adtran Netvanta 3305 VPN

Vínculos relacionados

Documentación de instalación en la página 83
Firmware de teléfonos VPN remote compatible en la página 83
Configuración del teléfono IP para el control remoto VPN en la página 84
Teléfonos IP y VLAN en la página 84
VLAN y DHCP en la página 86
Configuración de ejemplo: descripción general en la página 87
Descripción general del sistema de ejemplo en la página 89

Documentación de instalación

Este documento sólo cubre notas y diferencias específicas de la instalación de los teléfonos VPNremote con IP Office. Luego, la instalación y configuración de los teléfonos VPNremote de Avaya están cubiertas en varios documentos existentes disponibles a través del sitio web de asistencia técnica de Avaya (http://support.avaya.com). Consulte el documento de *Guía de configuración de VPN para teléfonos IP de la serie 9600* con referencia *16-602968*.

Vínculos relacionados

Teléfonos VPN Remote en la página 82

Firmware de teléfonos VPN remote compatible

A menos que se recomiende lo contrario, sólo deberá utilizarse el firmware proporcionado en el DVD de aplicaciones de administrador de IP Office para los teléfonos VPNremote conectados a una IP Office. Ese firmware está probado con la versión de IP Office para garantizar un funcionamiento correcto. El firmware se encuentra en un archivo comprimido en la carpeta `\bin\VPN Phone`.

Si bien puede ser que Avaya ponga a disposición otras versiones de firmware VPNremote para su descarga, es posible que esas versiones no hayan sido probadas específicamente con IP Office.

Vínculos relacionados

Teléfonos VPN Remote en la página 82

Configuración del teléfono IP para el control remoto VPN

Acerca de esta tarea

Además, se puede acceder a una opción de casilla de verificación Teléfono VPN permitido a través de la ficha de configuración **Extensión** > **VoIP** de las extensiones IP. La casilla de verificación **VoIP** se utiliza para indicar a IP Office qué extensiones que son VPNremote y que por lo tanto requieren el uso de una licencia.

Procedimiento

1. Utilizando IP Office Manager, recupere la configuración del sistema.
2. Haga clic en **Extensión** y seleccione la entrada de la extensión IP.
3. Seleccione la ficha **VoIP**.
4. Habilite **Teléfono VPN permitido**.
5. Haga clic en **Aceptar**.
6. Repita este proceso para cualquier otra extensión IP existente que se convertirá a una conexión VPN.
7. Guarde la configuración.

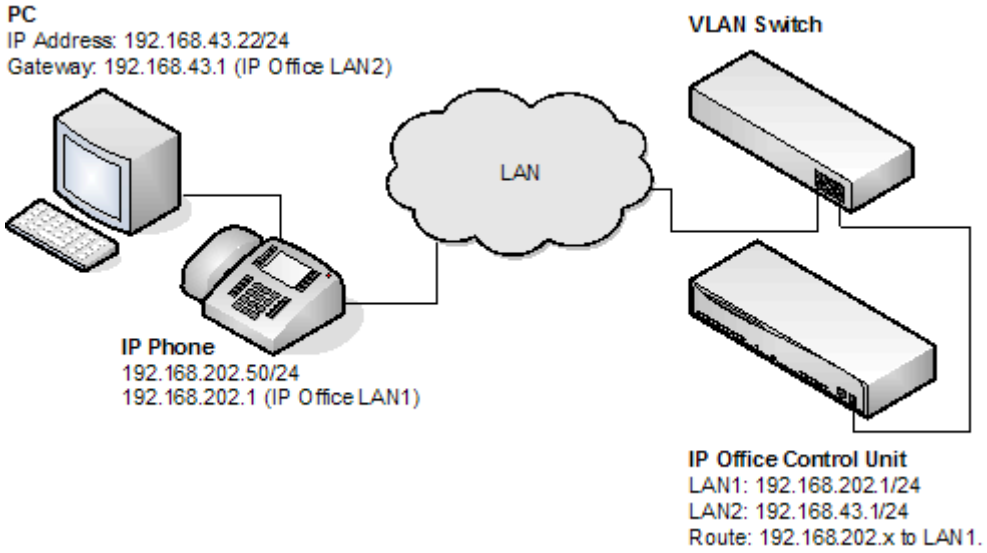
Vínculos relacionados

Teléfonos VPN Remote en la página 82

Teléfonos IP y VLAN

El uso de VLAN permite crear dominios de colisión separados en los conmutadores Ethernet. En el caso de los teléfonos IP e IP Office las ventajas son:

- Permite que las PC continúen en la misma subred IP mientras que los teléfonos IP pueden utilizar un esquema de direcciones IP nuevo e independiente.
- El tráfico de difusión no se propaga entre la red de datos de la PC y la red de voz de los teléfonos IP. Esto ayuda al desempeño ya que de lo contrario el tráfico de difusión debe ser evaluado por todos los receptores.
- La priorización del tráfico y las redes VLAN en la capa 2 se unen estrechamente en el mismo estándar 802.2. Por lo tanto, es más fácil mantener L2 QoS cuando se utiliza una red VLAN.



La tabla muestra las tres formas en las que VLAN puede utilizarse con un conmutador Ethernet. Los primeros dos métodos sólo requieren una configuración básica y como este documento supone que la PC y los teléfonos IP comparten el mismo puerto Ethernet, la atención se centrará en el tercer método (superposición).

Tipo	Descripción	Ventajas	Desventajas
Sin VLAN	Tanto la voz como los datos ocupan el mismo dominio de colisión	Configuración simple	Efecto adverso del tráfico de difusión de la PC sobre el tráfico de voz. Requiere dos (2) puertos por usuario, uno para el teléfono IP y el otro para la PC
VLAN física	VLAN independiente para datos y voz	Configuración simple	Requiere dos (2) puertos en el conmutador, uno para el teléfono IP y el otro para la PC
VLAN superpuesta	Un solo puerto en el conmutador que transporta el tráfico de la PC y los teléfonos IP	Requiere un solo puerto para la PC y el teléfono IP El tráfico de difusión de la PC no puede tener un efecto adverso sobre el tráfico de voz	Configuración compleja

Vínculos relacionados

Teléfonos VPN Remote en la página 82

VLAN y DHCP

El uso de VLAN tiene repercusiones en DHCP si DHCP se utiliza para permitir el uso de los teléfonos IP y/o las PC. La tabla que figura a continuación contiene información sobre las opciones disponibles cuando se utiliza un solo puerto para las PC y los teléfonos IP en una red habilitada para VLAN.

Opción de DHCP	Descripción
Ninguna (dirección fija)	Configuración manual de cada teléfono IP
Servidores DHCP independientes	Dos PC, una para cada red VLAN
Servidor DHCP con varias direcciones IP	Una sola PC con dos tarjetas NIC, una para cada VLAN
Relé DHCP	La opción debe ser compatible con el conmutador Ethernet

Si se utiliza DHCP, cuando el teléfono IP lo inicia primero realiza una solicitud de DHCP sin una etiqueta VLAN.

- Si la respuesta de DHCP contiene una nueva configuración VLAN como parte del alcance SSON, los teléfonos liberarán todas su direcciones IP existentes y hará una nueva solicitud DHCP usando el ID de VLAN recientemente suministrado

  Si el teléfono IP no consigue un nuevo ID de VLAN, continuará con la configuración provista en la respuesta DHCP original

También puede pasarse un ID de VLAN a un teléfono a través del archivo de configuración que carga. Nuevamente, el teléfono IP liberará todos sus parámetros IP existentes y luego harán una nueva solicitud usando el ID de VLAN suministrado recientemente.

En el ejemplo de abajo, cuando los teléfonos IP reciben una respuesta DHCP desde el servidor DHCP en la red VLAN de datos, esa respuesta contiene el ID de VLAN de la red VLAN de voz. Luego, el teléfono libera la configuración de VLAN de datos originales que obtuvo y envía una nueva solicitud DHCP a la red VLAN de voz.

Opción	Configuración de DHCP de la red VLAN de datos	Configuración de DHCP de la red VLAN de voz
Dirección IP	192.168.43.x	192.168.202.x
Máscara	255.255.255.0	255.255.255.0
Enrutador	192.168.43.1	192.168.202.1
SSON Alcance	L2Q=1, L2QVLAN=202, VLANTEST=0	MCIPADD=192.168.202.1, MCPORT=1719, HTTPSRVR=192.168.202.X VLANTEST=0
El parámetro VLANTEST es la cantidad de tiempo que el teléfono IP debe hacer solicitudes DHCP en una red VLAN (0 significa tiempo ilimitado).		

Vínculos relacionados

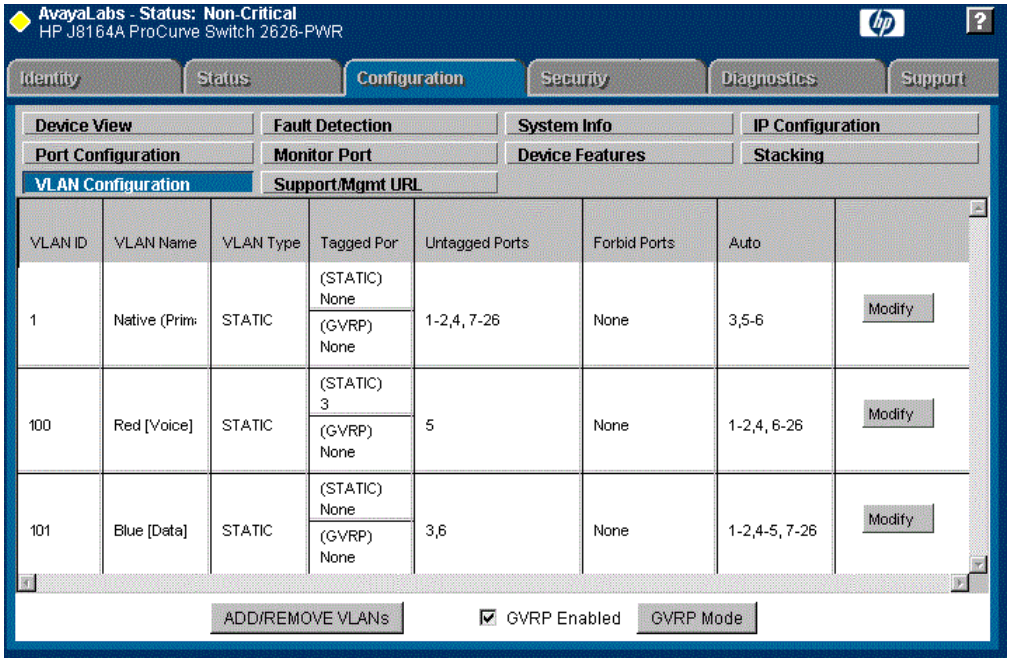
Teléfonos VPN Remote en la página 82

Configuración de ejemplo: descripción general

La red se ha creado para permitir que la PC del usuario se conecte al puerto conmutador del teléfono IP. Por lo tanto, un sólo cable conecta la PC y el teléfono IP al conmutador Ethernet. A los efectos de este ejemplo, VLAN 100 se utiliza para el tráfico de voz y VLAN 101 para el tráfico de datos. La interfaz LAN1 de la unidad de control de IP Office reside en la red VLAN de voz mientas que la interfaz LAN2 reside en la red VLAN de datos. La comunicación entre las redes VLAN de voz y datos se facilitan por la función del enrutador de la unidad de control de IP Office.

Conmutador HP: configuración

A continuación figura la configuración de CLI y Web del conmutador HP Procurve. Esto se obtiene mediante las pautas de configuración que pueden encontrarse más abajo.



HP Procurve CLI output

```
; J8164A Configuration Editor; Created on release #H.08.60

hostname "AvayaLabs"
snmp-server community "public" Unrestricted
vlan 1
name "Native"
untagged 1-2,4,7-26
ip address 192.168.202.201 255.255.255.0
no untagged 3,5-6
exit
vlan 100
name "Red [Voice]"
untagged 5
tagged 3
exit
vlan 101
name "Blue [Data]"
untagged 3,6
exit
gvrp
spanning-tree
```

La tabla que figura a continuación resume la configuración de HP para los puertos y redes VLAN.

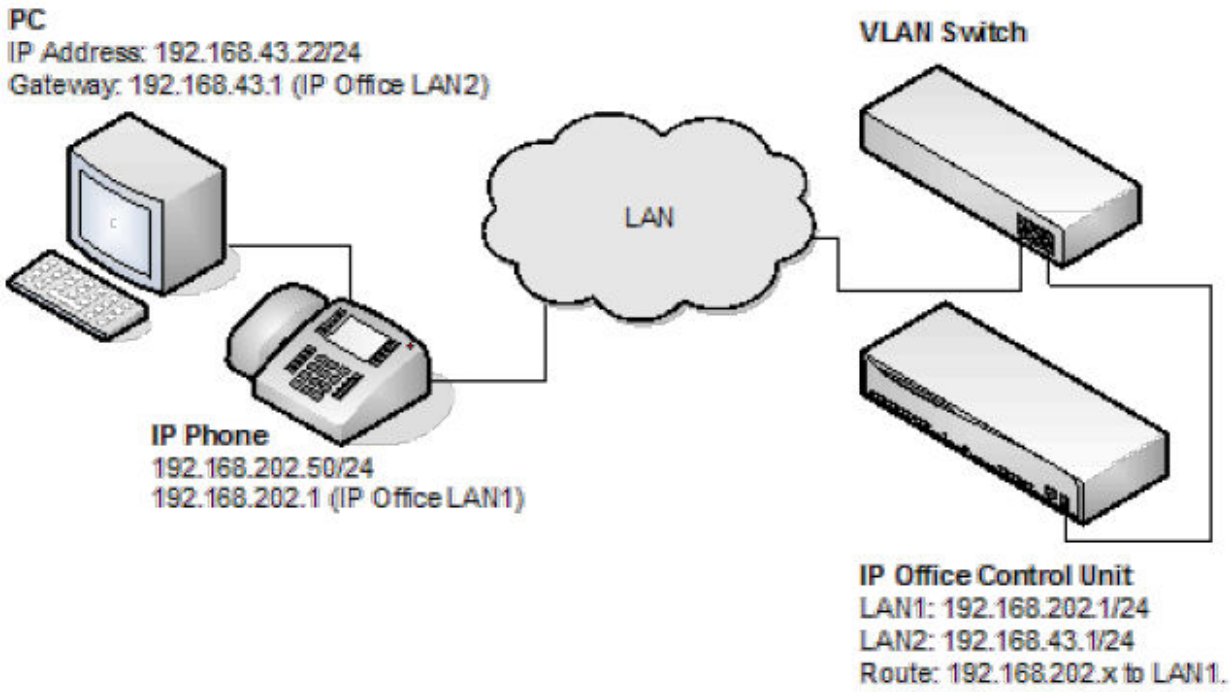
Puerto	VLAN 100 de voz	VLAN 101 de datos	Descripción
3	Etiquetado	No etiquetado	Este puerto se agregó tanto a la red VLAN 100 como la VLAN 101. **Nota:** Al añadir el puerto 3 a la red VLAN 100, debe etiquetarse la opción Modo, pero hay que quitar la etiqueta cuando se añade a la red VLAN 101.
5	No etiquetado	-	Este puerto sólo se incluye en VLAN 100 y no se incluye en VLAN 101. La opción Modo debe definirse como No etiquetada para el puerto 5 de esta red VLAN.
6	-	No etiquetado	El puerto 6 sólo se incluye en VLAN 101 y no se incluye en VLAN 100. La opción Modo DEBE definirse como No etiquetada para esta red VLAN.

El funcionamiento de la red depende de la funcionalidad definida en la documentación de HP. Específicamente, HP hace referencia a este tipo de funcionamiento de VLAN como **VLAN superpuesta**.

Vínculos relacionados

Teléfonos VPN Remote en la página 82

Descripción general del sistema de ejemplo



- Configuración de IP Office: la siguiente tabla detalla la configuración para IP Office. IP Office no requiere ninguna configuración adicional para la compatibilidad con el etiquetado 802.1.

Opción	Valor
LAN1 de dirección IP	192.168.202.1
LAN1 de máscara IP	255.255.255.0
LAN2 de dirección IP	192.168.43.1
LAN2 de máscara IP	255.255.255.0
Enrutador	192.168.202.1
Servidor de llamadas	192.168.202.1

- Configuración de teléfono IP: en el ejemplo a continuación, el teléfono IP se configuró con una dirección IP fija.

Opción	Valor
Dirección IP	192.168.202.50
Máscara IP	255.255.255.0
Enrutador	192.168.202.1
Servidor de llamadas	192.168.202.1
VLANID	100

- Configuración del conmutador VLAN: la tabla que figura a continuación resume la configuración de HP para los puertos y redes VLAN.

Puerto	VLAN 100 de voz	VLAN 101 de datos
3	Etiquetado	No etiquetado
5	No etiquetado	-
6	-	No etiquetado

- Configuración de la PC: a continuación figura la configuración IP de la PC1; no existe ninguna opción compatible con 802.1p o 802.1q habilitada en la PC.

Opción	Valor
Dirección IP	192.168.43.22
Máscara IP	255.255.255.0
Enrutador	192.168.43.1

Resumen

Desde el puerto en el que residen la PC y el teléfono IP, pueden recibirse dos tipos de marcos Ethernet (es decir, enviados desde el teléfono o la PC).

- El teléfono IP envía paquetes etiquetados.
- La PC envía paquetes no etiquetados.

Cuando la PC conectada al puerto del teléfono IP envía un paquete etiquetado, sólo se propagará a VLAN 101. Esto se debe a que al agregar el puerto 3 a VLAN 101, la opción **Modo** se especificó como no etiquetada. Mientras que para la otra red VLAN (101) la opción **Etiquetado** se seleccionó para el puerto 3 en VLAN 101. Los paquetes etiquetados se enviarán a VLAN 100 mientras que los no etiquetados se enviarán a 101.

Un paquete se etiqueta cuando se origina desde un teléfono IP. Dado que la opción "no etiquetada" se seleccionó para el puerto 5 de VLAN 100, la etiqueta 802.1 se eliminará antes de que el conmutador envíe el paquete a este puerto. Del mismo modo, cuando un paquete no etiquetado es originado y enviado por IP Office, el conmutador etiquetará el paquete antes de enviar el puerto LAN 3.

Vínculos relacionados

Teléfonos VPN Remote en la página 82

Capítulo 15: Configuración de un servidor DHCP alternativo

El método de instalación recomendado para los teléfonos IP H.323 utiliza un servidor DHCP. Esta sección describe, por medio de un ejemplo, los pasos básicos para utilizar un servidor Windows como servidor DHCP para la instalación de teléfonos IP. Los principios para definir un alcance son aplicables a la mayoría de los servidores DHCP.

Deberá obtener la información que se detalla a continuación del administrador de red del cliente:

- El intervalo de direcciones IP y la máscara de subred que los teléfonos IP H.323 deben utilizar.
- La dirección de la puerta de enlace IP
- El nombre de dominio DNS, la dirección del servidor DNS y la dirección del servidor WINS
- El tiempo de la concesión DHCP
- La dirección IP de la unidad IP Office
- La dirección IP de la PC que ejecuta la aplicación Manager (esta PC actúa como un servidor de archivos para los teléfonos IP H.323 durante la instalación).

Vínculos relacionados

Opciones alternativas en la página 91
Verificación de compatibilidad con servidor DHCP en la página 93
Creación de un alcance en la página 94
Incorporación de una opción 242 en la página 95
Activación del alcance en la página 96

Opciones alternativas

En este documento, toda la información de los teléfonos IP se emite a través de la configuración de la opción 176 o 242 y el alcance. Dependiendo del servidor DHCP, es posible que sea necesario utilizar otras opciones dentro del alcance.

Opción	Descripción
Opción 1: máscara de subred	

La tabla continúa…

Opción	Descripción
Opción 3: dirección IP de Gateway	Si se utiliza más de una dirección , la lista completa puede contener un total de hasta 255 caracteres ASCII. Debe separar las direcciones IP con comas y sin espacios.
Opción 6: direcciones de los servidores DNS	Si se utiliza más de una dirección , la lista completa puede contener un total de hasta 127 caracteres ASCII. Debe separar las direcciones IP con comas y sin espacios. Al menos una dirección de la opción 6 debe ser una dirección decimal válida, que no sea cero.
Opción 15: nombre de dominio DNS	Esta cadena contiene el nombre de dominio que debe utilizarse cuando las direcciones IP se determinen a partir de los nombres DNS de los parámetros del sistema. Este nombre de dominio se agrega al nombre DNS antes de que el teléfono IP intente determinar la dirección DNS. La opción 15 es necesaria si desea utilizar un nombre DNS para el servidor HTTP.
Opción 51: tiempo de arrendamiento de DHCP	Si esta opción no se recibe, la oferta de DHCP no debe aceptarse. Avaya recomienda un tiempo de arrendamiento de seis (6) semanas o más. Si esta opción tiene un valor de FFFFFFFF hexadecimal, se supone que el arrendamiento de la dirección IP es infinito según RFC 2131, sección 3.3, de modo tal que los procedimientos de renovación y revinculación no serán necesarios incluso si se reciben las opciones 58 y 59. El vencimiento de los arrendamientos provoca el reinicio de los teléfonos IP de Avaya. • Proporcione arrendamientos suficientes para que la dirección IP de un teléfono IP no cambie si se desconecta por un corto período. • El estándar de DHCP establece que cuando se produce el vencimiento de un arrendamiento de DHCP, el uso de la dirección IP asignada al dispositivo debe interrumpirse de inmediato. Si la red tiene problemas y el único servidor DHCP es centralizado, el teléfono no podrá acceder al servidor. En este caso, el teléfono no podrá utilizarse hasta que pueda establecer una conexión con el servidor. • Una vez que se haya asignado una dirección IP, el teléfono continúa utilizando esa dirección después del vencimiento del arrendamiento de DHCP, hasta que se detecte un conflicto con otro dispositivo. El parámetro DHCPSTD personalizable de los teléfonos IP de la serie 1600 permite que un administrador especifique que el teléfono: - Cumpla con el estándar DHCP estableciendo DHCPSTD en 1. - Continúe utilizando su dirección IP después del vencimiento del arrendamiento de DHCP estableciendo DHCPSTD en 0. Esta es la configuración predeterminada. Si se utiliza, una vez que el arrendamiento de DHCP haya vencido, el teléfono enviará una solicitud ARP por su propia dirección IP cada cinco (5) segundos. Esta solicitud continuará para siempre o hasta que el teléfono reciba una respuesta ARP. Una vez que haya recibido una respuesta ARP, el teléfono mostrará un mensaje de error, configurará la dirección IP como 0.0.0.0 e intentará volver a comunicarse con el servidor DHCP.
Opción 52: opción de sobrecarga	Si esta opción se recibe a través de un mensaje, el teléfono interpretará los campos de nombre y archivo de acuerdo con IETF RFC 2132, sección 9.3, que figuran en el Apéndice B: Documentación relacionada.
Opción 53: tipo de mensaje de DHCP	El valor es 1 (DHCPDISCOVER) o 3 (DHCPREQUEST).

La tabla continúa…

Opción	Descripción
Opción 55: lista de solicitudes de parámetros	Los calores aceptables son: 1 (máscara de subred), 3 (direcciones IP de enrutadores), 6 (direcciones IP de servidores de nombres de dominio), 15 (nombre de dominio), NVSSON (número de opción específico del sitio).
Opción 57: tamaño máximo de mensaje de DHCP.	Utilizado por un cliente o servidor DHCP para especificar el tamaño máximo del mensaje DHCP que está dispuesto a aceptar.
Opción 58: tiempo de renovación del arrendamiento de DHCP	Si no se recibe o si este valor es superior al correspondiente a la opción 51, el valor predeterminado de T1 (temporizador de renovación) se utilizará según IETF RFC 2131, sección 4.5.
Opción 59: tiempo de revinculación del arrendamiento de DHCP	Si no se recibe o si este valor es superior al correspondiente a la opción 51, el valor predeterminado de T2 (temporizador de revinculación) se utilizará según IETF RFC 2131, sección 4.5.

Nota:

En teléfonos IP H323, la configuración de la opción 66 será anulada por cualquier entrada TFTP de la opción 176. El uso de la opción 66 como parte del alcance se útil si se requieren direcciones de Gatekeeper alternativas en la configuración de la opción 176 a la vez que se respeta el límite de 127 caracteres.

Vínculos relacionados

Configuración de un servidor DHCP alternativo en la página 91

Verificación de compatibilidad con servidor DHCP

Procedimiento

1. En el servidor, seleccione **Comenzar** > **Programas** > **Herramientas administrativas** > **Administración del equipo**.
2. En **Servicios y aplicaciones**, en el Árbol de administración de la computadora, ubique **DHCP**.
3. Si DHCP no existe, deberá instalar los componentes de DHCP. Consulte la documentación de Microsoft.

Pasos siguientes

Si el rol del servidor DHCP es compatible, la primera etapa consiste en crear un alcance de direcciones para usar con teléfonos IP.

Vínculos relacionados

Configuración de un servidor DHCP alternativo en la página 91

Creación de un alcance

Acerca de esta tarea

Un alcance de DHCP define las direcciones IP que el servidor DHCP puede emitir en respuesta a las solicitudes DHCP. Pueden definirse diferentes alcances para distintos tipos de dispositivos.

Procedimiento

1. Vaya a **Comenzar** > **Programas** > **Herramientas administrativas** > **DHCP**.
2. Haga clic con el botón secundario en el servidor y seleccione **Nuevo** > **Alcance**.
3. Se iniciará el asistente de creación de alcance. Haga clic en **Siguiente**.
4. Ingrese un nombre y un comentario para el alcance y haga clic en **Siguiente**.
5. Ingrese el intervalo de direcciones que debe utilizarse, por ejemplo de 200.200.200.1 a 200.200.200.15 (recuerde que la parte del host no puede ser 0).
6. Ingrese la máscara de subred como la cantidad de bits utilizados o la máscara real, por ejemplo, 24 es igual a 255.255.255.0 y haga clic en **Siguiente**.
7. Puede especificar las direcciones que deben excluirse. Para hacer esto, puede ingresar un rango y hacer clic en **Agregar**.

   Puede ingresar el rango de 200.200.200.5 a 200.200.200.7

   Nota:

   Debe excluir IP Office de este intervalo, ya que las Opciones de DHCP de IP Office deben deshabilitarse. Esto es sólo una recomendación. Para lograr esto también puede dejar direcciones disponibles fuera del rango del alcance.
8. Haga clic en **Siguiente**.
9. Establezca el tiempo de arrendamiento para las direcciones.

   Si el tiempo es demasiado extenso, las direcciones utilizadas por los dispositivos que ya no estén conectados no se vencerán y estarán disponibles para volver a utilizarse en un período de tiempo razonable. Esto reduce la cantidad de direcciones disponibles para nuevos dispositivos. Si es demasiado corto, generará un tráfico innecesario para las renovaciones de direcciones. La opción predeterminada es 8 días.
10. Haga clic en **Siguiente**.
11. El asistente permite configurar las opciones de DHCP más frecuentes. Seleccione **Sí** y luego haga clic en **Siguiente**.
12. Ingrese la dirección de la puerta de enlace y haga clic en **Agregar**.
13. Haga clic en **Siguiente**.
14. Ingrese el dominio DNS (por ejemplo, example.com) y las direcciones del servidor DNS y haga clic en **Siguiente**.
15. Ingrese las direcciones del servidor WINS y haga clic en **Agregar** y luego haga clic en **Siguiente**.
16. A continuación, se le preguntará si desea activar el alcance. Seleccione **No** y luego haga clic en **Siguiente**.

17. Haga clic en **Terminar**.

Resultado

El nuevo alcance ahora aparecerá en la lista y el estado se configura en **Inactiva**.

Tras haber creado el alcance que usarán los teléfonos IP , debe agregarse un conjunto de opciones que concuerden con los números de opción específicos del sitio (SSON) que usará el sistema. De manera predeterminada, el SSON que usan los teléfonos de la serie 1600 y 9600 es 242.

Vínculos relacionados

Configuración de un servidor DHCP alternativo en la página 91

Incorporación de una opción 242

Acerca de esta tarea

Además de emitir la información de la dirección IP, los servidores DHCP pueden emitir otra información en respuesta a las solicitudes de diferentes números de opciones de DHCP específicas. La configuración de cada opción se adjunta al alcance. Los teléfonos IP H.323 series 1600 y 9600 usan SSON 242 para solicitar información adicional de un servidor DHCP. La opción debe incluir la definición de la dirección de gatekeeper H.323 del teléfono (la unidad de IP Office) y la dirección del servidor de archivos HTTP.

Procedimiento

1. Haga clic con el botón secundario en el servidor DHCP.
2. En el menú emergente, seleccione **Opciones predefinidas**.
3. Seleccione **Agregar**.
4. Introduzca la información que se indica a continuación:
   a. En **Nombre**, ingrese `16xxOptions`.
   b. En **Tipo de datos**, ingrese `Cadena`.
   c. En **Código**, ingrese `242`.
   d. En **Descripción**, ingrese la `configuración del teléfono IP`.
5. Haga clic en **Aceptar**.
6. En el campo de valor de cadena, ingrese `MCIPADD=xxx.xxx.xxx.xxx,MCPORT=1719,HTTPSRVR=yyyy.yyy.yyy.yyy,HTTPDIR=z, VLANTEST=0`.

   - Las cadenas pueden tener un máximo de 127 caracteres. Para reducir la longitud, la dirección del servidor TFTP puede especificarse a través de la incorporación de una entrada de la opción 66 en el alcance. Vea Opciones alternativas en la página 91.

     `MCIPADD=` es la dirección de Gatekeeper (Callserver) de H.323. Por lo general, esta es la dirección LAN1 de la unidad de IP Office. Puede ingresar varias direcciones IP, cada una separada por una coma y sin espacios. Esto permite especificar un gatekeeper de H.323 alternativo. Los teléfonos esperarán tres (3) minutos antes de

pasar a la alternativa y no volverán a cambiar cuando se recupere el primer servidor, hasta que el teléfono se reinicie.

- `MCPORT=` es la dirección del puerto RAS para iniciar el registro de los teléfonos. El valor predeterminado es 1719.
- `HTTPSRVR=` es la dirección IP del servidor de archivos HTTP.
- `HTTPDIR=`el directorio de archivos HTTP donde están ubicados los archivos del teléfono IP. Esta entrada no es necesaria si esos archivos se encuentran en el directorio raíz del servidor.

7. Haga clic en **Aceptar**
8. Para expandir el servidor, haga clic en el carácter [+] situado junto a él.
9. Haga clic en el alcance que acaba de crear para los teléfonos 1600 y 9600.
10. En el panel derecho, haga clic con el botón secundario en el alcance y seleccione **Opciones de alcance**.
11. En la ficha General, asegúrese de que 242 se encuentre marcada.
12. Verifique que el valor de cadena sea correcto y haga clic en **Aceptar**.

Pasos siguientes

Tras haber creado una opción 242 y asociado con el alcance que queremos que usen los teléfonos IP, ahora necesitamos activar el alcance.

Vínculos relacionados

Configuración de un servidor DHCP alternativo en la página 91

Activación del alcance

El alcance puede activarse manualmente si se hace clic con el botón secundario en el alcance, se selecciona **Todas las tareas** y se selecciona **Activar**. La activación será inmediata.

Podrá iniciar la instalación de los teléfonos IP H.323 mediante DHCP. Si la aplicación Manager se utiliza como el servidor HTTP o TFTP, asegúrese de que se esté ejecutando en la PC especificada.

Vínculos relacionados

Configuración de un servidor DHCP alternativo en la página 91

Capítulo 16: Compatibilidad con SRTP

En IP Office versión 9.1, se admite SRTP.

- Modos IP Office compatibles: SRTP es compatible con todos los modos IP Office.
- Teléfonos compatibles: se puede aplicar a extensiones SIP y H323. Sin embargo, existen restricciones para ciertos modelos específicos de teléfonos IP.
  - Compatible con H323 en teléfonos de la serie 9608, 9611, 9621 y 9641.
  - Compatible con SIP en teléfonos de Avaya y de terceros.
- Líneas troncales compatibles: puede aplicarse a todos los tipos de líneas IP (SIP, SM e IP Office (SCN)), excepto las troncales H323 externas.
- Licencias y capacidad: la utilización de SRTP no requiere de una licencia o suscripción. Sin embargo, la utilización de SRTP afecta la capacidad de llamadas del sistema.
  - En el caso de los sistemas IP500 V2/IP500 V2A con tarjetas VCM IP500, estas tarjetas se utilizan para admitir SRTP y reducir el impacto en la capacidad de llamadas del sistema. Esto no se aplica a las tarjetas de combinación.

Vínculos relacionados

Habilitación de SRTP del sistema en la página 97
Medios directos en la página 99

Habilitación de SRTP del sistema

De manera predeterminada, todas las líneas y extensiones IP están configuradas para que coincidan automáticamente con la configuración del sistema de nivel superior para SRTP, esté habilitado o deshabilitado. Esto simplifica la habilitación de SRTP al asegurar que todos los dispositivos utilizan la misma configuración de SRTP. Con este enfoque, una vez que SRTP está habilitado, la única configuración que se requiere en el nivel del dispositivo es deshabilitar SRTP en aquellas líneas o dispositivos para los que no es necesario.

Las líneas SIP son una excepción a esta regla, ya que para ellas SRTP está deshabilitado de manera predeterminada. Esto se debe a la escasa cantidad de proveedores de líneas SIP que actualmente admiten SRTP. Sin embargo, las líneas SIP pueden configurarse para que también se ajusten a la configuración en el nivel del sistema, si fuera necesario.

Vínculos relacionados

Compatibilidad con SRTP en la página 97
Habilitación del sistema SRTP en la página 98
Desactivación de SRTP en una extensión o línea en la página 98

Habilitación del sistema SRTP

Procedimiento

1. Obtenga la configuración del sistema.
2. Haga clic en **SISTEMA** y seleccione la ficha **Seguridad VoIP**.
3. Para **Seguridad de medios**, seleccione el nivel de funcionamiento de STRP que desee:

Configuración	Descripción
Desactivado	STRP no se utiliza para las conexiones.
Mejor esfuerzo	Admite RTP y SRTP. Use SRTP si se puede negociar una configuración SRTP que coincida con el extremo remoto. Esto requiere que el extremo remoto admita srtp rfc5939 (negociación de la funcionalidad para SRTP). De lo contrario, utilice RTP. Tenga en cuenta que los teléfonos E129 no admiten la opción **Mejor esfuerzo**.
Exigido	Utilice solo SRTP. No se permite la llamada si la sección remota no admite el SRTP coincidente.
Configuración avanzada	Una vez que seleccione la opción **Mejor esfuerzo** o **Exigido** como método de STRP, se recomienda que todos los demás ajustes de configuración de SRTP conserven sus valores predeterminados. La configuración predeterminada de suites criptográficas y marcas de SRTP se eligió de modo tal que funcionen con todos los dispositivos SIP y Avaya H323. Por ejemplo, la mayoría de las implementaciones de Avaya no admiten el cifrado RTCP y los teléfonos Avaya H323 solo admiten la suite criptográfica SHA_80.

4. Haga clic en **Aceptar**.

Vínculos relacionados

Habilitación de SRTP del sistema en la página 97

Desactivación de SRTP en una extensión o línea

Procedimiento

1. Haga clic en **Extensión** o **Línea** y seleccione la extensión o línea que desee.
2. Seleccione la ficha **VoIP**.
3. Cambie la configuración **Seguridad de medios** a **Desactivado**.
4. Haga clic en **Aceptar**.

Pasos siguientes

Repita esto para cualquier otra extensión o línea para la que no debería usarse SRTP.

Vínculos relacionados

Habilitación de SRTP del sistema en la página 97

Medios directos

Si se configuran medios directos, el sistema intenta negociar los medios directos entre los extremos de la llamada. Cuando hay un SRTP, además de revisar los criterios de VoIP coincidentes (por ejemplo, la compatibilidad de los códecs coincidentes), el sistema también revisa la configuración avanzada de seguridad de los medios y Seguridad de los medios correspondientes (las marcas de SRTP y suites criptográficas). Cualquier incompatibilidad prohíbe la llamada que usa medios directos.

Las llamadas entre secciones configuradas en distintos niveles de **Seguridad de medios** (**Desactivado**, **Mejor esfuerzo** o **Exigido**) no utilizarán medios directos.

Vínculos relacionados

Compatibilidad con SRTP en la página 97

Capítulo 17: Compatibilidad con TLS

En el caso de IP Office versión 10 y superior, es posible usar TLS para la conexión de los teléfonos 9600. Cuando está habilitada, la función TLS se usa para la señalización de llamadas y RAS de TCP entre el teléfono y el sistema IP Office.

- Compatible con los modelos 9608, 9611, 9621 y 9641.
- Requiere que el teléfono ejecute el firmware 6.6029 o superior.
- Requiere que el teléfono use una contraseña CRAFT no predeterminada.
- El uso de TLS por parte del sistema pueda configurarse como opcional o exigido.

Resumen del proceso

1. Personalización de la contraseña de proceso Craft
2. Adición de un certificado de identidad
3. Habilitar TLS en el sistema IP Office.
4. Habilitación de TLS en el teléfono

Notas adicionales

Para teléfonos con TLS:

- La conexión del servidor de archivos HTTPS utiliza el puerto 8411. El servidor de archivos necesita el mismo certificado.
- Si es remota y también utiliza SRTP, el teléfono usa el puerto 8443 para el respaldo o la restauración.

Vínculos relacionados

Cambio de contraseña CRAFT en la página 101
Adición del certificado de identidad en la página 101
Descargar del certificado de identidad desde un servidor basado en Linux en la página 102
Carga de un certificado en el almacén de certificados de confianza del servidor en la página 102
Habilitación de TLS en IP Office en la página 103
Habilitación de TLS en el teléfono en la página 103
Verificación del funcionamiento de TLS en la página 104

Cambio de contraseña CRAFT

Acerca de esta tarea

La configuración de operación de TLS del teléfono no puede modificarse si los teléfonos están usando la contraseña de proceso CRAFT predeterminada. La contraseña puede cambiarse de la siguiente manera:

Procedimiento

1. Si los teléfonos descargan un archivo `46xxsettings.txt` de un servidor de archivos, haga lo siguiente:
   a. Agregue una entrada **SET PROCPSWD** al archivo `46xxsettings.txt` después de la contraseña que debería usarse.
   b. Reinicie los teléfonos para cargar la nueva configuración.
2. Si los teléfonos utilizan la configuración generada automáticamente de IP Office:
   a. Obtenga la configuración de IP Office y ubique el usuario **NoUser**.
   b. En la ficha **Números de origen**, agregue **SET_46xx_PROCPSWD** seguido de la nueva contraseña.

      Tenga en cuenta que el comando distingue mayúsculas de minúsculas.
   c. Guarde la configuración y reinicie el sistema.
3. Para ver la configuración del archivo generado automáticamente:
   a. Abra el navegador e ingrese `http://<server_address>/46xxsettings.txt`.
   b. En el archivo, incluya una línea que comience **SET PROCPSWD** seguida de la nueva contraseña.

Vínculos relacionados

Compatibilidad con TLS en la página 100

Adición del certificado de identidad

De manera predeterminada, se utiliza el certificado raíz de IP Office. Para un IP500 V2, este es su propio certificado de seguridad autofirmado y no se requieren otros cambios. Para los servidores basados en Linux, es necesario descargar el certificado autofirmado propio del servidor y luego cargarlo en el almacén de certificados de confianza del servicio de IP Office.

Para usar el certificado de un tercero, dicho certificado debe cargarse en el almacén de certificados de confianza de IP Office.

Se informa al teléfono sobre el certificado que debe usarse al configurar el archivo `46xxsettings.txt` que recibe. Se utilizan los siguientes ajustes de configuración:

- `SET TLSSRVRVERIFYID 1`: esta configuración le indica al teléfono que verifique el certificado TLS.
- `SET TRUSTCERTS Root-CA-xxxxxxxx.pem`: esta configuración indica el nombre del certificado de seguridad que el teléfono debe solicitar y cargar al iniciarse.

Cuando IP Office recibe una solicitud de un certificado, busca en su almacén de certificados de confianza. Si los bytes 13-16 de la clave pública de la CA raíz coincide con xxxxxxxx del nombre del archivo de la solicitud, IP Office proporciona la CA raíz como archivo generado automáticamente con el nombre `Root-CA-xxxxxxxx.pem`.

Para los sistemas que utilizan archivos generados automáticamente, la configuración se agrega automáticamente. En el caso de otra instalación, la configuración debe agregarse manualmente a la sección del archivo 46xxsettings para los teléfonos 9608, 9611, 9621 y 9641.

Vínculos relacionados

Compatibilidad con TLS en la página 100

Descargar del certificado de identidad desde un servidor basado en Linux

Acerca de esta tarea

Procedimiento

1. Navegue hasta https://%3Cserver_address%3E:7071 e inicie sesión en los menús de Web Control del servidor.

   O bien, inicie sesión en los menús de administración web del servidor y luego seleccione **Vista de plataforma**.
2. Seleccione la ficha **Configuración** y después seleccione **General**.
3. Ubique la sección **Certificados**.
4. En la sección **Configuración de autoridad certificada (CA)**, haga clic en **Descargar (con codificación PEM)**.

Vínculos relacionados

Compatibilidad con TLS en la página 100

Carga de un certificado en el almacén de certificados de confianza del servidor

Procedimiento

1. Inicie IP Office Manager.
2. Seleccione **Archivo** > **Avanzada** > **Configuración de seguridad**.
3. Seleccione el servidor e inicie sesión.
4. Seleccione **SISTEMA**.
5. Seleccione la ficha **Certificados**.
6. En la sección **Depósito de certificados de confianza**, haga clic en **Agregar**.

Vínculos relacionados

Compatibilidad con TLS en la página 100

Habilitación de TLS en IP Office

Acerca de esta tarea

El sistema IP Office puede utilizar una cantidad de opciones TLS.

Procedimiento

1. Con IP Office Manager, cargue la configuración del servidor.
2. Seleccione **SISTEMA**.
3. Seleccione la ficha **LAN1** o **LAN2**, según corresponda y, luego, la ficha **VoIP**.
4. El funcionamiento de TLS es controlado por el campo **Señalización H.323 por TLS**. Seleccione el modo de TLS que desee:
   - **Desactivado**: no utilice TLS. Los teléfonos configurados para TLS recurren a la conexión de TCP normal.
   - **Preferido**: utilice TLS con teléfonos configurados para TLS pero también permita las conexiones de TCP normales desde otros teléfonos.
   - **Exigido**: requiere TLS. Rechace las conexiones desde teléfonos que no están configurados para TLS. Tenga en cuenta que, cuando está opción está seleccionada, el **Puerto de señalización de llamada remota** está fijado en 1300.
5. Haga clic en **Aceptar**.
6. guarde los cambios en la configuración. Deje que el sistema se reinicie.

Vínculos relacionados

Compatibilidad con TLS en la página 100

Habilitación de TLS en el teléfono

Acerca de esta tarea

Se accede a la configuración de TLS para el teléfono a través del menú Depuración.

Nota:

Cuando los teléfonos existentes se actualizan al firmware compatible con TLS, se habilita de manera predeterminada la configuración Señalización de H.323 por TLS. Sin embargo, con los sistemas que no están configurados para el funcionamiento de TLS, los teléfonos recurren a la conexión de TCP.

Procedimiento

1. Presione **SILENCIAR** después de la contraseña de proceso CRAFT y #.

Puede acceder al menú en los teléfonos usando la contraseña de proceso CRAFT predeterminada. Sin embargo, en tal caso solo podrá ver la configuración, pero no podrá cambiarla.

2. Desplácese y seleccione **DEPURACIÓN**.
3. Desplácese hasta **Señalización H.323 por TLS**.
4. Cambie la configuración según sea necesario.
5. Haga clic en **Guardar**.
6. Haga clic en **Salir**.

Resultado

El teléfono se reiniciará usando los nuevos valores de configuración.

Vínculos relacionados

Compatibilidad con TLS en la página 100

Verificación del funcionamiento de TLS

El uso de TLS puede verificarse y confirmarse de la siguiente manera:

- System Status Application: los detalles de **Extensión** indican qué **Protocolo de capa 4** utiliza la conexión de la extensión. **TLS** se muestra cuando se utiliza TLS.
- Control del sistema: dentro del control, seleccione **Estado** > **Estado del teléfono H323**. La **Transporte**columna muestra **TLS** para extensiones que usan TLS para su conexión.

  En los datos de monitor, los registros Tx y Rx RAS H323 indican si utilizan TLS. De manera similar, los registros CS y RAS H323 muestran el uso del puerto 1300.

Vínculos relacionados

Compatibilidad con TLS en la página 100

Parte 5: Misceláneo

Capítulo 18: Opciones de administración fija

A través del teléfono pueden modificarse determinados valores de configuración después de la instalación. Estos procedimientos sólo deben utilizarse si utiliza la instalación de dirección fija. No use estos procedimiento si está utilizando DHCP, excepto si está intentando reasignar un teléfono que se ha instalado anteriormente de forma estática.

Para definir parámetros para todos los teléfonos IP H.323 en un sistema, puede editar el archivo de comandos `46xxsettings.txt`. Sin embargo, los valores asignados a través de la administración fija anulan cualquier valor asignado a través del archivo 46xxsettings.txt. Permanecen activos para el teléfono IP hasta que se descargue un nuevo archivo de inicio.

Vínculos relacionados

Uso de opciones de administración fija en la página 106
Contraseña del proceso del administrador en la página 108
Habilitación de la interfaz de concentrador en la página 108
Ver detalles del teléfono en la página 110
Procedimiento de autocomprobación para teléfonos de la serie 1600 en la página 112
Procedimiento de autocomprobación para teléfonos de la serie 9600 en la página 113
Restablecimiento de un teléfono en la página 113
Eliminación de un teléfono en la página 114
Número de opción específico del sitio en la página 115

Uso de opciones de administración fija

El método que usa para acceder a administración fija depende del tipo de teléfono. Para acceder a muchas de las funciones de administración fija deben utilizarse secuencias de teclas para lo que primero se debe presionar **SILENCIAR** o **RET**. En versiones de firmware recientes se ha dado preferencia al uso de **SILENCIAR** y algunos teléfonos, como por ejemplo los de la serie 1600, solo admiten la opción **SILENCIAR**.

Vínculos relacionados

Opciones de administración fija en la página 106
Ingreso de opciones administrativas en teléfonos de la serie 1600 en la página 107
Ingreso de opciones administrativas en teléfonos de la serie 9600 en la página 107

Ingreso de opciones administrativas en teléfonos de la serie 1600

Acerca de esta tarea

Esta sección describe cómo ingresar datos para las opciones administrativas.

Procedimiento

1. Con el teléfono inactivo, presione **SILENCIAR**.

   Una vez que presione **SILENCIAR**, si no se presiona un botón válido en un lapso inferior a seis (6) segundos con respecto al botón anterior, los dígitos recopilados se descartan y el teléfono vuelve al estado inactivo.
2. Marque la contraseña de proceso administrativo.
3. Marque los dígitos para el comando que desee y luego #.
   - Los intentos de ingresar datos válidos se rechazarán y el teléfono emitirá un tono de error.
   - Si se ingresa un dígito numérico para un valor o para un campo de una dirección IP o máscara de subred después de sólo ingresar un cero, el nuevo dígito reemplazará el cero.
   - Para avanzar al próximo paso, presione #.

Vínculos relacionados

Uso de opciones de administración fija en la página 106

Ingreso de opciones administrativas en teléfonos de la serie 9600

Acerca de esta tarea

Solo es posible acceder a los procedimientos administrativos para los teléfonos de la serie 9600 reiniciando el teléfono.

Procedimiento

1. Con el teléfono colgado e inactivo, presione `MUTE <password> #`.
2. Desplácese por el menú hasta la acción necesaria y selecciónela.

   Cuando concluye el procedimiento seleccionado, el teléfono volverá al menú de procedimientos.
3. Cuando se hayan completado todos los procedimientos necesarios, presione **Salir**.

Resultado

El teléfono se reinicia con la nueva configuración.

Vínculos relacionados

Uso de opciones de administración fija en la página 106

Contraseña del proceso del administrador

Acerca de esta tarea

Los procesos telefónicos administrativos están protegidos por el uso de una contraseña del proceso, también conocida como contraseña CRAFT. Es posible cambiar la contraseña predeterminada y especificar un nuevo valor en el archivo `46xxsettings.txt`.

Procedimiento

1. Si los teléfonos descargan un archivo `46xxsettings.txt` de un servidor de archivos, haga lo siguiente:
   a. Agregue una entrada **SET PROCPSWD** al archivo `46xxsettings.txt` después de la contraseña que debería usarse.
   b. Reinicie los teléfonos para cargar la nueva configuración.
2. Si los teléfonos utilizan la configuración generada automáticamente de IP Office:
   a. Obtenga la configuración de IP Office y ubique el usuario **NoUser**.
   b. En la ficha **Números de origen**, agregue **SET_46xx_PROCPSWD** seguido de la nueva contraseña.

      Tenga en cuenta que el comando distingue mayúsculas de minúsculas.
   c. Guarde la configuración y reinicie el sistema.
3. Para ver la configuración del archivo generado automáticamente:
   a. Abra el navegador e ingrese `http://<server_address>/46xxsettings.txt`.
   b. En el archivo, incluya una línea que comience **SET PROCPSWD** seguida de la nueva contraseña.

Vínculos relacionados

Opciones de administración fija en la página 106

Habilitación de la interfaz de concentrador

La interfaz de concentrador se encuentra en muchos teléfonos IP Avaya que pueden usarse para conexión de PC de usuario. La interfaz de concentrador está habilitada de manera predeterminada.

Vínculos relacionados

Opciones de administración fija en la página 106
Habilitación de la interfaz de concentrador para teléfonos de la serie 1600 en la página 109
Habilitación de la interfaz de concentrador para la serie 9600 en la página 109

Habilitación de la interfaz de concentrador para teléfonos de la serie 1600

Procedimiento

1. Con el teléfono colgado e inactivo, presione `MUTE <password> INT #` o `MUTE <password> 468 #`.

   Los valores de configuración del puerto del teléfono aparecen en una secuencia. Las opciones varían entre los diferentes modelos de teléfono.

   - `PHY2=`

     Es la toma LAN de la conexión de la PC identificada como en el teléfono. Presione 1 ó 0 para habilitar o inhabilitar la interfaz hub respectivamente. Para continuar, presione #.

   - `IR=`

     Es el puerto infrarrojo (IR) situado en la parte delantera de algunos teléfonos IP H.323. Presione 1 ó 0 para habilitar o inhabilitar la interfaz hub respectivamente. Para continuar, presione #.

2. Presione # para guardar los nuevos valores.

Resultado

Aparecerá el mensaje `Los valores nuevos se están guardando` y el teléfono volverá a funcionar normalmente.

Vínculos relacionados

Habilitación de la interfaz de concentrador en la página 108

Habilitación de la interfaz de concentrador para la serie 9600

Procedimiento

1. Con el teléfono colgado e inactivo, presione `MUTE <password> #`.
2. Desplácese por el menú hasta **INT**.
3. Seleccione el puerto que desea ajustar. Las opciones son **Ethernet** y **Ethernet PC**.
4. Use los botones < y > para desplazarse a través de las posibles configuraciones de los puertos.

   La opción adicional **Desactivado** está disponible para el puerto Ethernet de la PC.

5. Presione **Guardar**.
6. Seleccione otro procedimiento o presione **Salir** para reiniciar el teléfono.

Vínculos relacionados

Habilitación de la interfaz de concentrador en la página 108

Ver detalles del teléfono

Puede ver una cantidad de detalles del teléfono. Esta información se agrega a la dirección fija y las opciones de administración local que también pueden utilizarse para evaluar la configuración.

Vínculos relacionados

Opciones de administración fija en la página 106
Ver detalles de los teléfonos de la serie 1600 en la página 110
Visualización de detalles de teléfonos de la serie 9600 en la página 111

Ver detalles de los teléfonos de la serie 1600

Procedimiento

1. Con el teléfono está colgado e inactivo, presione `MUTE CRAFT VIEW #` o `MUTE 27238 8439 #`.
2. Para mostrar la información, presione * en cualquier momento durante la visualización. Se muestra la siguiente configuración:

Valor	Descripción
Modelo	Muestra el número de modelo del teléfono, como por ejemplo 4624D02A.
Mercado	Muestra 1 para exportación o 0 para EE. UU. No aparece en todos los tipos de teléfonos.
Nº serie tel	Muestra el número de serie del teléfono.
Nº serie PWB	Muestra el **número de serie de tarjeta de circuitos impresos** del teléfono.
Código de componente de tarjeta de circuitos impresos (PWB)	Muestra el código de componente de tarjeta de circuitos impresos (PWB).
Dirección MAC	Muestra la dirección MAC del teléfono como números hexadecimales combinados.
Etiquetado L2	Indica si el etiquetado L2 está **activado**, **desactivado** o configurado como **automático**.
ID VLAN	Se utiliza para el teléfono. El valor predeterminado es 0.
dirección IP	La dirección IP asignada al teléfono.
Máscara de subred	La máscara de subred asignada al teléfono.
Enrutador	La dirección del enrutador asignada al teléfono.
Servidor de archivos	La dirección del servidor de archivos asignado al teléfono.
Servidor de llamadas	La dirección de Gatekeeper del teléfono H.323.
802.1X	La configuración actual para el funcionamiento 802.1X, si se utiliza.

La tabla continúa…

Valor	Descripción
Grupo	Esto muestra el valor de grupo definido en el teléfono. Los valores de grupo pueden utilizarse para controlar qué opciones (tanto firmware como valores de configuración) descarga un teléfono.
Protocolo	Mostrar **predeterminado**.
filename1 (nombre de archivo1)	Muestra el nombre del archivo de la aplicación del teléfono en la memoria del teléfono. Son valores del archivo de inicio que se cargó y no el nombre de archivo real.
Ethernet de 10MBps **Ethernet de 100Mbps**	Muestra la velocidad de la conexión LAN detectada.
filename2 (nombre de archivo2)	Muestra el nombre del archivo de inicio y la versión. Son valores del archivo de inicio que se cargó y no el nombre de archivo real.

3. Para finalizar el procedimiento y restablecer la interfaz de usuario a su estado anterior, presione #.
4. Para mostrar el siguiente valor presione *.

Vínculos relacionados

Ver detalles del teléfono en la página 110

Visualización de detalles de teléfonos de la serie 9600

Procedimiento

1. Con el teléfono colgado e inactivo, presione `MUTE <password> #`.
2. Desplácese hasta el menú **VER** e inicie el procedimiento.

Valor	Descripción
Modelo	Muestra el número de modelo del teléfono, como por ejemplo 4624D02A.
Nº serie tel	Muestra el número de serie del teléfono.
Nº serie PWB	Muestra el **número de serie de tarjeta de circuitos impresos** del teléfono.
Código de componente de tarjeta de circuitos impresos (PWB)	Muestra el código de componente de tarjeta de circuitos impresos (PWB).
MAC	Muestra la dirección MAC del teléfono como números hexadecimales combinados.
Grupo	Muestra el valor de grupo configurado en el teléfono. Los valores de grupo pueden utilizarse para controlar qué opciones (tanto firmware como valores de configuración) descarga un teléfono.
Protocolo	Mostrar **predeterminado**.

La tabla continúa…

Valor	Descripción
Archivo de la aplicación	Muestra el nombre del archivo de la aplicación del teléfono en la memoria del teléfono. Son valores del archivo de inicio que se cargó y no el nombre de archivo real.
Ethernet	Muestra la velocidad de la conexión LAN detectada.
Archivo de arranque	Muestra el nombre del archivo de inicio y la versión. Son valores del archivo de inicio que se cargó y no el nombre de archivo real.
Servidor proxy	Muestra la información del servidor proxy seleccionado.
Archivo de idioma de voz	El nombre del archivo de idioma que está usando el teléfono. Este está en blanco cuando se usa el idioma predeterminado del teléfono (inglés).

3. Presione **Volver**.
4. Seleccione otro procedimiento o presione **Salir** para reiniciar el teléfono.

Vínculos relacionados

Ver detalles del teléfono en la página 110

Procedimiento de autocomprobación para teléfonos de la serie 1600

Procedimiento

1. Para iniciar el procedimiento de autocomprobación del teléfono IP, presione `MUTE <password> TEST #` o `MUTE <password> 8378 #`.

   El teléfono hará lo siguiente:

   - Cada columna de indicadores LED de botones programables se enciende por medio segundo de izquierda a derecha en el teléfono, en un ciclo repetido. Los indicadores LED de altavoz/mudo y de mensaje en espera también se encienden en una secuencia.
   - Los botones (con excepción de #) generan un clic si se los presiona.
   - Los teléfonos con pantallas muestran `Self test #=end`(Autocomprobación #=finalización) durante 1 segundo después del inicio de la autocomprobación. A continuación, aparece un carácter de bloque (todos los píxeles encendidos) en todas las ubicaciones de caracteres de la pantalla durante cinco (5) segundos. La visualización del carácter/bloque se utiliza para encontrar píxeles de pantalla dañados.
   - Si la autocomprobación se aprueba:

     ```
     Self test passed
     #=end
     ```

   - Si la autocomprobación no se aprueba:

     ```
     Self test failed
     #=end
     ```

2. Para finalizar la autocomprobación, presione #.

Resultado

El teléfono volverá a funcionar normalmente.

Vínculos relacionados

Opciones de administración fija en la página 106

Procedimiento de autocomprobación para teléfonos de la serie 9600

Procedimiento

1. Con el teléfono colgado e inactivo, presione `MUTE <password> #`.
2. Desplácese por el menú hasta **Probar**.
3. Presione **Probar** nuevamente para confirmar la acción.

Vínculos relacionados

Opciones de administración fija en la página 106

Restablecimiento de un teléfono

Al restablecer un teléfono se restablecen todos los valores del sistema y la mayoría de los valores de inicialización del sistema. El procedimiento no afecta los datos y la configuración específica del usuario (por ejemplo, Datos de contacto, Configuraciones de opciones, extensión o contraseña de inicio de sesión, etc.). Para eliminar todos estos datos, consulte Eliminación de un teléfono en la página 114.

Vínculos relacionados

Opciones de administración fija en la página 106
Restablecimiento del teléfono de la serie 1600 en la página 113
Restablecimiento del teléfono de la serie 9600 en la página 114

Restablecimiento del teléfono de la serie 1600

Procedimiento

1. Con el teléfono colgado e inactivo, presione la siguiente secuencia: `MUTE <password> RESET #`

   `MUTE <password> 73738 #`

   Advertencia:

   Cuando presione #, toda la información fija se eliminará sin ninguna posibilidad de recuperar los datos.
2. Para continuar, presione #.

Cuando que se restablezcan los valores predeterminados del sistema, aparecerá Restauración de valores.

Una vez que los valores del sistema se hayan restablecido, aparecerá el mensaje `¿Desea reiniciar el teléfono?`.

3. Para finalizar el procedimiento sin reiniciar el teléfono, presione *.
4. Para reiniciar el teléfono, presione #.

   El resto de procedimiento dependerá del estado de los archivos de inicio y de la aplicación. Vea Escenarios de reinicio en la página 117.

Vínculos relacionados

Restablecimiento de un teléfono en la página 113

Restablecimiento del teléfono de la serie 9600

Procedimiento

1. Con el teléfono colgado e inactivo, presione `MUTE <password> #`.
2. Desplácese por el menú y seleccione **Restablecer valores**.
3. Presione **Restablecer** para confirmar la acción.

Resultado

Se restablecen las configuraciones de usuario del teléfono y se reinicia el teléfono.

Vínculos relacionados

Restablecimiento de un teléfono en la página 113

Eliminación de un teléfono

La eliminación de todos los valores de inicialización del sistema y su restauración a su configuración predeterminada y la eliminación de todos los datos específicos del usuario están destinados principalmente a la reparación y el uso cuando se entrega el teléfono a un nuevo usuario. Esto permite que el teléfono regrese a un estado cerca del original. El teléfono aún conservará los archivos de firmware que ya descargó.

Nota:

Es posible configurar algunos parámetros, como los clics de botones, los tonos de error y los timbres personalizados para un usuario específico a través del MENU. Estas configuraciones de usuario se restaurarán al registrar al usuario con el teléfono, ya que dichos parámetros se configuran en IP Office. Todas las otras configuraciones (por ejemplo, Datos de contacto, Configuraciones de opciones, etc.) se eliminan del teléfono.

Vínculos relacionados

Opciones de administración fija en la página 106
Eliminación de teléfonos de la serie 1600 en la página 115
Eliminación de teléfonos de la serie 9600 en la página 115

Eliminación de teléfonos de la serie 1600

Procedimiento

1. Mientras el teléfono está colgado e inactivo, presione la siguiente secuencia `MUTE <password> CLEAR #`.

   `MUTE <password> 25327 #`

2. Para continuar, presione #.

   Advertencia:

   Cuando presione #, toda la información fija se eliminará sin ninguna posibilidad de recuperar los datos.

   Cuando que se restablezcan los valores predeterminados del sistema, aparecerá`Eliminación de valores`.

Resultado

Una vez que se borran todos los valores, el teléfono se reinicia como si fuera un teléfono nuevo.

Vínculos relacionados

Eliminación de un teléfono en la página 114

Eliminación de teléfonos de la serie 9600

Procedimiento

1. Con el teléfono colgado e inactivo, presione `MUTE <password> #`.
2.
3. Desplácese por el menú y seleccione **Borrar**.
4. Presione **Borrar** nuevamente para confirmar la acción.

Resultado

Se eliminan las configuraciones y se reinicia el teléfono.

Vínculos relacionados

Eliminación de un teléfono en la página 114

Número de opción específico del sitio

Los teléfonos IP utilizan el número de opción específico del sitio (SSON) para solicitar información a un servidor DHCP que es específico de los teléfonos y no de otros dispositivos IP compatibles con el servidor DHCP. El número debe coincidir con una opción con una "opción" con un número similar establecido en el servidor DHCP que define los diversos valores de configuración requeridos por el teléfono.

El SSON predeterminado que usan los teléfonos de la serie 1600 y 9600 de Avaya es 242. Para teléfonos que son compatibles con DHCP de IP Office, el SSON que usa el teléfono debe coincidir con uno de los números opcionales específicos para el sitio que se establecen en la configuración de IP Office.

Advertencia:

Esto no debe realizarse si se utilizan direcciones fijas. El procedimiento sólo debe llevarse a cabo si se utiliza una dirección de DHCP y si se modificó el valor predeterminado normal del número de opción de DHCP.

Vínculos relacionados

Opciones de administración fija en la página 106
SSON en teléfonos de la serie 1600 en la página 116
SSON en la serie de teléfonos 9600 en la página 116

SSON en teléfonos de la serie 1600

Procedimiento

1. Con el teléfono colgado e inactivo, presione `MUTE <password> SSON` o `MUTE <password> 7766 #`.

   SSON= aparece seguido del valor actual.

2. Ingrese el nuevo valor. Debe ser un número entre 128 y 255.
3. Para cancelar el procedimiento, presione * o bien # para guardar el nuevo valor.

Vínculos relacionados

Número de opción específico del sitio en la página 115

SSON en la serie de teléfonos 9600

Procedimiento

1. Con el teléfono colgado e inactivo, presione `MUTE <password> #`.
2. Desplácese hasta el menú **SSON** e inicie el procedimiento.
3. Ingrese el nuevo número SSON que debe usar el teléfono cuando se reinicie la próxima vez.
4. Presione **Guardar**.
5. Seleccione otro procedimiento o presione **Salir** para reiniciar el teléfono.

Vínculos relacionados

Número de opción específico del sitio en la página 115

Capítulo 19: Escenarios de reinicio

Lasecuencia del proceso de reinicio depende de la versión del archivo de inicio del teléfono que ya se descargó en el teléfono así como de la del servidor de archivos. Este apéndice explica los diferentes escenarios posibles.

Todos los procedimientos de inicio que se detallan a continuación implican los mismos pasos iniciales cuando el teléfono negocia con el servidor DHCP y el servidor de archivos.

1. Después de suministrar energía, el teléfono muestra el mensaje `Reiniciando` seguido de `Inicializando`.
2. Cuando el archivo de la aplicación (de haber uno) o el código de inicio se descomprime en la memoria RAM, aparece el mensaje Cargando. Dado que esto demora un rato, aparecerán asteriscos, luego puntos y nuevamente asteriscos en la segunda línea para indicar que algo está sucediendo.
3. Cuando el control pasa al código contenido en la memoria RAM, aparece el mensaje `Iniciándose`.
4. El teléfono detecta y muestra la velocidad de la interfaz Ethernet en Mbps (que es 10 ó 100). El mensaje Sin Ethernet significa que la velocidad de la interfaz LAN no puede determinarse. La velocidad Ethernet indicada es la velocidad de la interfaz LAN para el teléfono y cualquier PC conectada.
5. DHCP aparece cuando el teléfono obtiene una dirección IP y otra información del servidor DHCP de LAN. La cantidad de segundos transcurridos aumenta hasta que la configuración de DHCP se haya completado con éxito.
   - Si el teléfono se configuró con una dirección fija (para lo que se presiona * cuando aparece DHCP), se omitirá DHCP y se utilizará la configuración de la dirección fija que se obtuvo.
   - Es importante señalar que cargar un nuevo archivo de inicio en cualquier momento borrará toda la información de las direcciones fijas.
6. Una vez que DHCP se ha completado exitosamente, el teléfono solicita archivos del servidor de archivos que se indica en la respuesta de DHCP. El primer archivo solicitado detalla los otros archivos que el teléfono también debe cargar. Primero, el teléfono hace su solicitud de archivo usando HTTPS. Si esto falla, hace la misma solicitud usando HTTP. Si eso falla, hace una solicitud final usando TFTP. Si todas las solicitudes de un archivo fallan, el teléfono pasa a una alternativa usando la versión actual del archivo que tenga en su propia memoria.
7. Una vez que el archivo de comandos de actualización se haya cargado, la secuencia dependerá del estado de los archivos que actualmente se encuentran en la memoria del teléfono, en comparación con los incluidos en el archivo de comandos de actualización.

Vínculos relacionados

El archivo de inicio debe actualizarse en la página 118

No se encontró ningún archivo de la aplicación o el archivo de la aplicación debe actualizarse en la página 118
Los archivos correctos de inicio y de la aplicación ya se han cargado en la página 119

El archivo de inicio debe actualizarse

Después de procesar el archivo de comandos de actualización, el software determina que el nombre del archivo de código de inicio del teléfono no coincide con el archivo de comandos de actualización. El archivo de comandos especifica el nombre del nuevo archivo que debe cargarse.

1. El teléfono muestra el nombre de archivo y la cantidad de kilobytes que se cargó.
2. El teléfono muestra el mensaje `Saving to flash` mientras el nuevo archivo de inicio se almacena en la memoria Flash. Aparecerán el porcentaje del archivo almacenado y la cantidad de segundos que han transcurrido. Por lo general, esto demorará más tiempo del que se tardó para descargar el archivo.
3. El teléfono muestra el mensaje `Reiniciando` o mientras se prepara para reiniciarse mediante el nuevo archivo de inicio.
4. El teléfono muestra el mensaje `Inicializando`.
5. Mientras el nuevo archivo de inicio se descomprime en la memoria RAM, el teléfono muestra el mensaje `Cargando`. Dado que esto demora un rato, aparecerán asteriscos, luego puntos y nuevamente asteriscos en la segunda línea para indicar que algo está sucediendo.
6. Cuando el control pasa al software que acaba de descargarse, el teléfono muestra el mensaje `Iniciando`.
7. El teléfono muestra el mensaje `Borrando` mientras la memoria Flash se borra durante la preparación para volver a escribir el código. También aparecen el porcentaje de memoria que se borró y la cantidad de segundos que transcurrieron.
8. Aparece el mensaje Actualizándose mientras vuelve a escribirse el código de inicio. El teléfono también muestra el porcentaje del código de inicio reescrito y la cantidad de segundos transcurridos.
9. Cuando el nuevo código de inicio se haya escrito en la memoria Flash con éxito, el teléfono se reiniciará para que el estado de los archivos de la aplicación del teléfono puedan verificarse.

Vínculos relacionados

Escenarios de reinicio en la página 117

No se encontró ningún archivo de la aplicación o el archivo de la aplicación debe actualizarse

Esto sucede con las actualizaciones normales de los archivos de la aplicación. Después de procesar el archivo de comandos de actualización, el software determina que el nombre del

archivo de inicio del teléfono es la versión correcta. A continuación determina que el nombre del archivo de la aplicación no coincide con el almacenado en el teléfono.

1. El teléfono muestra el nombre de archivo requerido mientras descarga el archivo del servidor TFTP. También muestra la cantidad de kilobytes que se descargaron.
2. Aparece el mensaje `Guardando en la memoria`. También aparecerán en el teléfono el porcentaje del archivo almacenado y la cantidad de segundos que han transcurrido. Por lo general, esto demorará más tiempo del que se tardó para descargar el archivo.
3. El teléfono se reinicia para que pueda ejecutarse el archivo de la aplicación específico del sistema.

Vínculos relacionados

Escenarios de reinicio en la página 117

Los archivos correctos de inicio y de la aplicación ya se han cargado

Esto sucede con la mayoría de los reinicios normales. Después de procesar el archivo de comandos de actualización, el software determina que el nombre del archivo de inicio del teléfono y el archivo de la aplicación del teléfono coinciden con aquellos especificados en el archivo de comandos de actualización.

1. El registro específico del sistema con el conmutador del inicia. El teléfono solicita el número de extensión y la contraseña que debe utilizar.
   - De forma predeterminada, el teléfono muestra el último número de extensión que utilizó. Para aceptar, presione #.
   - Cuando aparece una solicitud de contraseña, la verificación de la contraseña no se lleva a cabo salvo si el usuario cambia el número de extensión.
   - Se verifica la contraseña sea la **Contraseña del teléfono** de la extensión almacenada en IP Office Manager. Si no se ha configurado un **Contraseña del teléfono**, el sistema también verificará el código de inicio de sesión del usuario que coincida. Los sistemas anteriores a IP Office versión 9.0 solo utilizan el **Código de inicio de sesión** del usuario que coincida.
2. Al concluir el registro, hay disponible un tono de marcación en el teléfono si también puede obtener una licencia de extensión o suscripción de usuario.

Vínculos relacionados

Escenarios de reinicio en la página 117

Capítulo 20: Recursos

Documentación

Búsqueda de documentos en el sitio web de Soporte técnico de Avaya

Procedimiento

1. Vaya a https://support.avaya.com.
2. En la parte superior de la pantalla, escriba su nombre de usuario y contraseña y haga clic en **Login**.
3. Haga clic en **Support by Product** > **Documents**.
4. En **Enter your Product Here**, escriba el nombre del producto y, a continuación, seleccione el producto de la lista.
5. En **Choose Release**, seleccione el número de versión apropiado.

   El campo **Choose Release** no está disponible si existe solo una versión para el producto.
6. En el filtro **Content Type**, haga clic en un tipo de documento, o haga clic en **Select All** para ver una lista de todos los documentos disponibles.

   Por ejemplo, para guías de usuario, haga clic en **User Guides** en el filtro **Content Type**. La lista muestra únicamente los documentos para la categoría seleccionada.
7. Haga clic en **Enter**.

Capacitación

Visualización de videos de orientación de Avaya

Los videos de orientación de Avaya proporcionan contenido técnico sobre cómo instalar, configurar y resolver problemas en los productos Avaya.

Acerca de esta tarea

Los videos están disponibles en el sitio web de soporte de Avaya, ubicados bajo el tipo de documentos de video, y en el canal de YouTube administrado por Avaya.

- Para encontrar videos en el sitio web de soporte de Avaya, vaya a https://support.avaya.com/ y realice una de las siguientes acciones:
  - En **Search**, escriba `Avaya Mentor Videos`, haga clic en **Clear All** y seleccione **Video** en **Content Type**.
  - En **Search**, escriba el nombre del producto. En la página **Search Results**, haga clic en **Borrar todo** y seleccione **Video** en **Content Type**.

    El tipo de contenido de **Video** se muestra únicamente cuando los videos están disponibles para ese producto.

  En el panel derecho, la página muestra una lista de videos disponibles.
- Para encontrar videos de orientación de Avaya en YouTube, vaya a www.youtube.com/AvayaMentor y realice una de las siguientes acciones:
  - Ingrese una o varias palabras clave en **Buscar Canal** para buscar un producto o tema específico.
  - Desplácese hacia abajo a **Listas de reproducción** y haga clic en el nombre del tema para ver la lista de videos disponibles para el tema. Por ejemplo, Contact Centers.

Nota:

No todos los productos tienen videos disponibles.

Soporte técnico

Vaya al sitio web de soporte técnico de Avaya en https://support.avaya.com si desea obtener la documentación más reciente, notificaciones sobre el producto y artículos de conocimientos. También puede buscar notas de publicación, descargas y soluciones a problemas. Utilice el servicio web de solicitud de servicios para crear una solicitud de servicio. Realice consultas a los agentes en directo o solicite que un agente lo comunique con el equipo de soporte técnico si un problema requiere conocimientos específicos adicionales.

Vínculos relacionados

Uso de Base de conocimiento de Avaya InSite en la página 121

Uso de Base de conocimiento de Avaya InSite

La Base de conocimientos de Avaya InSite es un motor de búsqueda web que provee:

- Procedimientos actualizados para solución de problemas y consejos técnicos
- Información sobre los service packs
- Acceso a documentación del cliente y técnica
- Información sobre programas de capacitación y certificación

- Vínculos a otra información pertinente

Si es un socio de Avaya autorizado o un cliente actual de Avaya con un contrato de soporte, puede acceder a la Base de conocimiento sin costo adicional. Debe tener una cuenta de inicio de sesión y un número Sold-To válido.

Use la Base de conocimiento Avaya InSite para buscar posibles soluciones a problemas.

1. Vaya a http://www.avaya.com/support.
2. Inicie sesión en el sitio web de Avaya con un usuario y una contraseña válidos.

   El sistema muestra la página de **Avaya Support**.
3. Haga clic en **Support by Product** > **Product-specific Support**.
4. En **Enter Product Name**, indique el producto y, luego, presione `Intro`.
5. En la lista, seleccione el producto y una versión.
6. Haga clic en la ficha **Technical Solutions** para ver los artículos.
7. Seleccione los artículos relevantes.

Vínculos relacionados

Soporte técnico en la página 121

Índice

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V