GUÍA DEL ADMINISTRADOR

Cisco Small Business

Configuration Assistant de Cisco Versión 3,0(1)
Sistema de comunicaciones de Smart Business
Guía del administrador

Número de revisión de documento 78-20226-01

Chapter 1: Aspectos básicos de Configuration Assistant de Cisco 15

Qué es Configuration Assistant de Cisco? 16
Requerimientos del sistema 17
Descarga e instalación de CCA 19
Verificando actualizaciones de aplicaciones para CCA 20
Verificación de la compatibilidad de la versión de CCA 20
Interfaz de usuario 21
Barra del menú 22
Barra de herramientas 25
Barra de funciones 27
Escritorio de CCA 29
Tablero 30
Vista Topología 34
Opciones de topología 42
Comentarios 44
Vista del panel frontal 44
Iconos y gráficos de estado de enlaces 47
Aplicar y guardar la configuración 50
Visualización y administración de errores 51
Mensajes de voz de advertencia 52
Configuración de preferencias 55
Notificación de mensajes del sistema 62
Crear o Modificar Notificaciones del sistema 63

Utilización de la ayuda en línea 64
Impresión de ventanas, informes y gráficos de CCA 66

Chapter 2: Novedades 67
Versión actual 67
Versiones recientes 68

Chapter 3: Guía de inicio de la configuración 79
Crear y administrar sitios de clientes 80
Acerca de los sitios de clientes 80
Planificación de sitios de clientes 81
Crear un nuevo sitio de clientes 85
Opciones de conexión 87
Modificar un sitio de cliente 88
Adgregar un dispositivo a un sitio de clientes existente 89
Visualización y listado de dispositivos en un sitio de clientes 89
Administración de los sitios de clientes 90
Conexión a un sitio o dispositivo autónomo 91
Utilización de Asistentes de configuración de CCA 94
¿Cuál Asistente debería usar y cuándo? 95
Asistente de configuración de telefonía 98
Asistente de configuración de seguridad 101
Asistente de configuración inalámbrica 104
Asistente de configuración de dispositivo 107
Utilidad de configuración para SR520-T1 108
Asistente de configuración de VPN de teléfonos 108
Asistente de configuración de monitoreo de vídeo 111
Copia de seguridad y restauración de configuración del dispositivo 119
Uso de CCA con Cisco Small Business Office Manager 122
Recursos para planificar e implementar su solución SBCS 122
Comunidad de soporte para pequeñas empresas de Cisco 123

Smart Designs de Cisco 124
Guías de referencia para plataformas UC540 y UC560 de Cisco 124
Funciones de SBCS de Cisco admitidas dentro de CCA 124

Chapter 4: Propiedades del dispositivo 127

Su nombre de host 127
Hora del sistema 128
Modificar hora del sistema 131
Servidor de tiempo de la red 132
Sincronizar hora del sistema 133
Zona horaria (Sólo dispositivos de seguridad SA500) 134
Puerto HTTP 136
Usuarios y contraseñas 137
Crear usuario 141
Modificar contraseña de usuario 142
Modificar habilitar contraseña 142
Acceso remoto a dispositivos (Telnet) 143
SNMP 143
Crear o Modificar filtro SNMP (serie ESW500) 147
Crear vista de SNMP 149
Modificar vista SNMP 149
Crear grupo SNMP 150
Modificar grupo SNMP 151
Crear usuario SNMP 152
Modificar usuario SNMP 153

Chapter 5: Configuración de puertos y switch 155

Configuración de puertos de switch 155
Modificar configuraciÃ³n de puerto 161
Modificar descripciones del puerto 161
Filtro 162

Smartports 162
Modificar perfiles de puerto 164
Detalles del rol de puerto 166
Smartports sugeridos 166
VLANs 168
Crear VLAN 171
Sincronización de VLAN 172
Reflejo de puertos (switches de la serie ESW500) 173
Spanning Tree Protocol (switches CE520) 175
Snooping IGMP (switches CE520) 178
Modificar Snooping IGMP 179
Direcciones MAC (switches CE520) 180
Ventana Búsqueda de puertos (switches CE520) 181
EtherChannels (switches CE520) 184
Crear grupos de puertos 187
Modificar grupos de puertos 188

Chapter 6: Conexiones de enrutamiento y redes 191

Direcciones IP 191
Conexión a Internet 196
Modificar conexión a Internet 199
Servidor DHCP 202
Crear Exclusión DHCP 205
Crear Conjunto DHCP 206
Modificar Conjunto DHCP 207
Crear Asociaciones DHCP 207
Modificar Asociación DHCP 208
Enrutamiento estático 208
Agregar ruta estática 209

Chapter 7: Inalámbrica 211

Configuración inalámbrica segura 211
Crear o Modificar SSID de WLAN 223
Opciones de seguridad inalámbrica para dispositivos AP541N 226
Opciones de seguridad inalámbrica para dispositivos UC500W y AP541N 230
Convertir a Punto de acceso liviano (LAP) 235
Configuración de conversión 237
Estado de la conversión 238
Configuración del controlador de LAN inalámbrica 239
Configuración de interfaces inalámbricas para un controlador de WLAN 240
Visualización de estado de clientes inalámbricos para un controlador de WLAN 242
Configuración de usuarios de WLAN 243
Proxy DHCP 250
Tablero del controlador inalámbrico 250
Configurar el servidor RADIUS para controladores de WLAN 252

Chapter 8: Funciones de seguridad 255

Traducción de direcciones de la red (NAT) 255
Visión general 256
Ventana NAT (Direcciones IP asignadas a través de DHCP) 257
Ventana NAT (IP estática o PPPoE con IP estática) 259
Servidor VPN 261
VPN remota 266
Agregar una red 268
Agregar una cuenta 269
Firewall y DMZ 269
Crear Servicio DMZ 273
Firewall - Editar ACL 273

Auditoría de seguridad 274
Configuración de seguridad de red (Switches CE520) 276
Agregar una dirección MAC 279
Modificar una dirección MAC 279
VPN SSL 280
Configurar lista de reenvío de puertos 289
Agregar una cuenta de usuario 290
Agregar sitios web de Intranet 291
Instalar ventana del software del cliente de la VPN SSL 291
Sistema de prevención de intrusiones (IPS) 292
Filtro de URL (serie SR500) 296

Chapter 9: Configuración de región y sistema de telefonía 299

Inicio del sistema de voz 299
Configuración del sistema de voz 300
Configuración regional para telefonía 302

Chapter 10: Puertos y enlaces de voz 305

Puertos FXS 305
Enlaces PSTN 307
Configuración de puertos FXO 313
Configuración 319
Descripción 319
Troncal SIP 322
Estado de enlace 327

Chapter 11: Usuarios y anexos 329

Usuarios y teléfonos 329
Anexos de usuarios 330
Anexos flotantes 342
Movilidad de anexos 345

Anexos analógicos 357
Configuración de asignaciones de botones de teléfonos 358
Correo de voz y notificaciones 377
Ubicación con número individual (SNR) 391
Agregar un usuario SNR 394
Modificación de un usuario SNR 395
Discados rápidos del sistema 397

Chapter 12: Grupos telefónicos 399

Grupos de llamado 399
Llamar a grupos de envío 402
Grupos de contestación 406
Grupos de localización 407
Vista Dependencia de grupo de localización 412

Chapter 13: Funciones de voz 415

Parqueo de llamadas 415
Creación o edición de una ranura de parqueo de llamadas 417
Conferencia 419
Conference Barge 422
Música en espera (MoH) 429

Chapter 14: Gestión de llamadas 431

Calendarios 431
Contestadora automática 435
Requisitos previos 435
Configuración de Contestadora automática 435
Solicitar Administración 440
Administración del archive de comandos 443
Distribución básica automática de llamadas (ACD) 444
Visión general 444

Antes de comenzar 445
Configure el servicio ACD básica 446
Crear/Editar parámetros de ACD básica 447
Miembros del grupo de búsqueda 450
Parámetros del informe del grupo de búsqueda 450
Atención nocturna 451
Teléfonos de Atención nocturna 454
Grabación en vivo 454
T.37 Facsímil a correo 457
Visión general 457
Limitaciones 458
Prerequisitos para configurar T.37 Facsímil 459
Activación de T.37 Facsímil a correo y configuración de servicios 460
Configuración de buzones de correo para los facsímiles entrantes 464

Chapter 15: Plan de numeración 467

Plan de numeración entrante 467
Discado directo a anexos de usuario interno 469
Discado directo a Contestadora automática, Grupos, Operadora 471
Plan de numeración saliente 473
Agregar ID de quien llama para los anexos internos 483
Parámetros del Grupo de enlaces 485

Chapter 16: Gestión del sitio 489

Administrador de múltiples sitios 489
Requisitos y pautas de diseño de múltiples sitios 490
Procedimientos de configuración de múltiples sitios 497
Requisitos previos para la configuración de múltiples sitios 498
Agregar y configurar sitios 499
Configuracion del sitio 506
Configuración de DDNS 509
Configuración de Calidad de servicio (QoS) 510

Exportación e importación de sitios 512
Modificación de un sitio después de su configuración inicial 514
Eliminación de un sitio 514
Monitoreo del estado de múltiples sitios 515
Funciones de voz admitidas en múltiples sitios 517
Máximo de llamadas (Control de admisión de llamadas) 518

Chapter 17: Aplicaciones 521

Configuración general 521
URL de autenticación 522
Acceso al menú de servicios 523
Cuentas de llamadas 525
Autenticación HTTPS 526
Administrador de Smart Applications 527
Configuración específica para la aplicación 528
Mensajería unificada (IMAP) 529
Vídeo Telefonía 529
PhoneConnect de WebEx de Cisco 530
TimeCardView 544

Chapter 18: Mantenimiento 549

Paquetes de localización y software para UC500 de Cisco 549
Paquetes de software de UC500 550
Paquetes de software para el UC500 551
Descarga de paquetes de localización y software para UC500 de Cisco 551
Ver información de versión de software y propiedades del dispositivo 552
Actualizaciones de software 552
Actualización del firmware del dispositivo 552
Instalación de software del UC500 556
Estado de actualización de software 558

Actualización de correo de voz (UC560) 559
Administración de licencias 562
Acciones de administración de licencias 567
Cargar archivo de licencias 571
Reiniciar / Restablecer dispositivos 572
Cómo localizar el UC500 (localizaciones diferentes a Inglés de EE.UU.) 573
Administración de archivos 574
Administración de cargas telefónicas 580

Chapter 19: Supervisar 585

Red 586
Estadísticas de puertos 586
Gráficos de ancho de banda 592
Gráficos de enlaces 594
Utilización inalámbrica 598
Estado T1/E1/BRI 599
DNS y Hosts 599
Seguridad 599
Estado de la red VPN 600
Telefonía 601
Inventario 605
Detalles de inventario 606
Registro del sistema 606
Estado de múltiples sitios 606
Estado 607
Detalles del estado 608
Notificación de eventos 610
Filtro de notificación 612
Mensajes del sistema 612
Filtro de mensajes del sistema 613

Chapter 20: Solución de problemas 615

Diagnóstico de circuitos (Retrobucle T1) 615
Diagnóstico de red 618
Hacer ping 618
Rastreo 619
Asociaciones DHCP 620
Estado del sistema 621
Registro de depuración de WAN (SR520-T1) 621
Diagnóstico de telefonía 623
Prueba del plan de numeración 623
Registro de enlaces SIP 625
Registro de solución de problemas de voz 627
Registro de depuración de teléfonos 629
Captura de PCM 631
Teléfonos analógicos SCCP 633
Diagnóstico de conectividad de CUE 634
Diagnóstico de seguridad 637
Registro de depuración de Firewall/NAT 637
Registro de depuración de VPN 639
Depuraciones genéricas 641
Comandos ejecutables de IOS 643
Comandos ejecutables de CUE 643
Generación de un registro de soluciones de problemas del sistema 644
Enlaces y Conectividad (switches CE520) 645

Appendix A: Dónde ir desde aquí 647

Glossary 649

Contenidos

1

Aspectos básicos de Configuration Assistant de Cisco

¡Bienvenido a Configuration Assistant de Cisco!

- Haga clic **aquí** para obtener instrucciones sobre cómo utilizar el sistema de ayuda.
- Consulte **Guía de inicio de la configuración, página 79** para las instrucciones sobre cómo crear sitios de cliente y utilizar asistentes de configuración de dispositivos incorporados.
- Consulte **Recursos para planificar e implementar su solución SBCS, página 122** para obtener información acerca de la comunidad de soporte de SBCS y recursos para socios.

Si no se conoce a Configuration Assistant (CCA) de Cisco, la información de las siguientes secciones le ayudará a comenzar:

- **Qué es Configuration Assistant de Cisco?**
- **Requerimientos del sistema**
- **Descarga e instalación de CCA**
- **Verificando actualizaciones de aplicaciones para CCA**
- **Verificación de la compatibilidad de la versión de CCA**
- **Interfaz de usuario**
- **Aplicar y guardar la configuración**
- **Visualización y administración de errores**
- **Mensajes de voz de advertencia**
- **Configuración de preferencias**
- **Notificación de mensajes del sistema**

- **Utilización de la ayuda en línea**
- **Impresión de ventanas, informes y gráficos de CCA**

Qué es Configuration Assistant de Cisco?

Configuration Assistant es una aplicación para administrar plataformas y dispositivos Small Business Pro de Cisco. Los dispositivos pueden administrarse como autónomos o en grupos de dispositivos, llamados *sitios de clientes*, desde cualquier lugar de su intranet. Con esta interfaz gráfica, usted podrá

- Configurar un sistema Smart Business Communications System (SBCS) de Cisco
- Configuraciónde conexiones de puertos
- Configurar las funciones de telefonía de su sitio de clientes
- Administrar las licencias de telefonía en los dispositivos de voz IP
- Configurar la traducción de direcciones de redes, redes privadas virtuales y firewalls
- Configurar las funciones LAN de inalámbricas de su sitio de clientes, incluyendo la seguridad inalámbrica y el acceso inalámbrico para invitados.
- Administrar y auditar la seguridad de la red
- Ver todo el sitio de clientes en un mapa de topología
- Ver los paneles frontales de los dispositivos admnistrados
- Supervisar el estado de los dispositivos, el ancho de banda y los enlaces
- Consultar informes de inventario y estadísticas
- Actualizar el software de los dispositivos
- Reiniciar dispositivos y restablecer los dispositivos a su configuración de fábrica por defecto
- Hacer copia de seguridad y restaurar la configuración del sitio

Para realizar cualquiera de estas tareas, seleccione la función adecuada de la barra de funciones de CCA, como se muestra en la **“Barra de funciones” section on page 27**.

Requerimientos del sistema

La PC en la que se instala CCA debe cumplir con los siguientes requisitos mínimos:

Requerimientos del sistema	
Sistemas operativos admitidos (Windows)	Microsoft Windows Vista Ultimate (edición de 32 bits ó 64 bits) Microsoft Windows XP Professional, Service Pack 2 ó posterior Microsoft Windows 7 (versiones de 64 bits y 32 bits) Se necesitará permiso por escrito hacia el directorio inicial y hacia el directorio de instalación para que CCA pueda crear los archivos de registro y de preferencias necesarios. Para las PC que ejecutan Windows Vista y Windows 7 se requieren privilegios de administrador para actualizar, instalar y usar CCA. Cuando se usa CCA en las PC que usan Microsoft Windows 7, configura la función de inactividad automática como Nunca. Para cambiar la configuración de la PC siga estos pasos: ▪ Vaya a **Panel de control** > **Opciones de energía.** Por defecto, está configurada como Balanceado. ▪ Haga clic en **Cambiar cuando la computadora pasa a inactividad** ▪ Aumente la configuración "Pasar a inactividad" desde 15 minutos (predeterminado) a **Nunca**

Requerimientos del sistema	
Soporte para Mac OS (requiere software de virtualización)	**Mac OS**: 10,5 y posterior **Virtual OS**: Parallels Desktop 3.0 y posteriores o VMware Fusion 1.0 y posteriores **Guest OS**: Microsoft Windows XP (Service Pack 2 ó posterior) o Microsoft Windows Vista Ultimate. CCA también admite control remoto por medio de clientes de Virtual Network Computing (VNC).
Hardware	PC con puerto LAN FastEthernet o superior
Procesador	1.8 GHz Intel Core 2 Duo o superior
Espacio en disco	400 MB recomendado
Memoria	1 GB mínimo, 2 GB recomendado
Pantalla	Resolución de pantalla: 1280 x 1024 o superior recomendado
Navegador	Se recomienda Microsoft Internet Explorer 8.0 o posterior, con Javascript activado. El plug-in de Adobe Flash Player 10 ó posterior para Microsoft Internet Explorer también debe estar instalado (además de cualquier otra versión del plug-in de Flash que pueda tener instalado para diferentes exploradores de internet. Javascript debe estar activado para el navegador Microsoft Internet Explorer.

Descarga e instalación de CCA

Para instalar CCA en su PC, haga lo siguiente:

PASO 1 Visite el siguiente sitio web: www.cisco.com/go/configassist.

Debe ser un usuario de Cisco.com registrado, pero no es necesario tener otros privilegios de acceso.

PASO 2 En el cuadro de información de soporte, haga clic en el enlace **Descargar software**.

PASO 3 Si ya no está registrado, se le redigirá a la página de inicio de sesión de Cisco.com. Especifique su nombre y contraseña de Cisco para iniciar sesión.

PASO 4 Busque el archivo del instalador de CCA; por ejemplo, `Cisco-config-assistant-win-k9-3_0-en.exe`).

PASO 5 Descargue el instalador de CCA y ejecútelo. Se puede ejecutar el instalador directamente desde Internet si su navegador permite esta opción.

CCA es gratuito; no hay cobros por descargarlo, instalarlo ni usarlo.

Cuando se ejecuta el instalador, siga las instrucciones de la pantalla. En la página final, haga clic en Configurar estos parámetros en la ficha Avanzadas.**Finalizar** para completar la instalación.

Si se está utilizando una versión más antigua de CCA, utilice la función de Actualizar aplicación para actualizarlo a la última versión. Consulte **“Verificando actualizaciones de aplicaciones para CCA” section on page 20**.

Una vez que CCA esté instalado, seleccione **Inicio** > **Todos los programas** > **Cisco Configuration Assistant** > **Cisco Configuration Assistant** o use el acceso rápido instalado para iniciar CCA.

Ya que CCA no está conectado a un sitio de clientes ni a un dispositivo, sólo unos pocos elementos del menú y la ventana Conectar están disponibles luego de iniciar CCA por primera vez. Cuando CCA no está conectado a un dispositivo ni a un sitio de clientes, la barra de menú y la barra de herramientas sólo admiten las tareas que personalizan a CCA. La barra de funciones, que por lo general muestra las funciones del dispositivo, está vacía.

Para conectarse a un dispositivo o crear un sitio de clientes, consulte **Crear y administrar sitios de clientes, página 80** y **Conexión a un sitio o dispositivo autónomo, página 91**.

Verificando actualizaciones de aplicaciones para CCA

Puede mantener CCA actualizado buscando e instalando las actualizaciones en Cisco.com.

Para usar la función de actualización automática, se debe iniciar sesión en Cisco.com.

Se le solicitará buscar una actualización si

- CCA encuentra un nuevo tipo de dispositivo o un dispositivo con un software actualizado entre los dispositivos que gestiona.
- Usted configura una búsqueda en la ventana Preferencias y el intervalo de tiempo ha expirado.
- La versión de CCA que se está usando es más antigua que la versión que se usó previamente para configurar el dispositivo o sitio de clientes al que se está conectando.

También se puede buscar una actualización a pedido seleccionando **Sistema** > **Actualizaciones de aplicación** en la barra de menú.

Si CCA encuentra una actualización, puede leer una descripción de sus contenidos y decidir si instalarla.

Verificación de la compatibilidad de la versión de CCA

Cuando se inicia CCA y se conecta a un dispositivo o sitio de clientes, y la versión de CCA que se está usando es anterior a la versión de CCA que se usó previamente para configurar ese dispositivo o sitio de clientes, aparece el diálogo Conflicto de versión de CCA.

El mensaje "La versión de la CCA que está utilizando es más antigua que la versión anterior que se utilizó para configurar este dispositivo. Esto puede ocasionar errores. Cisco recomienda enfáticamente\nque se actualice a CCA versión X.x ó posterior. Do you want to upgrade now?”

Si selecciona **Sí**, se le solicitará que especifique su nombre de usuario y contraseña de Cisco.com para acceder a las actualizaciones de la aplicación CCA.

Interfaz de usuario

La interfaz de usuario de CCA facilita la administración de las funciones de trabajo en redes y la solicitud de servicios desde CCA. Estas son las partes principales de la interfaz del usuario:

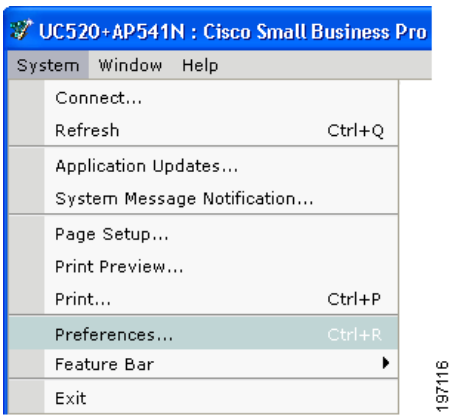
- **Barra de menú.** La fila de los menús en la parte superior de la ventana CCA. Ofrece servicios para las aplicaciones, una lista ventanas abiertas y ayuda en línea. Para saber más sobre la barra de menús, consulte **Barra del menú, página 22**.
- **Barra de herramientas.** La fila de iconos que aparece directamente bajo la barra de menú. Los iconos representan los servicios de aplicaciones usados con mayor frecuencia y las funciones de red configuradas más a menudo. Para aprender qué representa cada icono, consulte **Barra de herramientas, página 25**.
- **Espacio de trabajo.** El área principal de la ventana de CCA, todo lo que aparece entre la barra de herramientas y la barra de estado. Consta de dos partes, la barra de funciones y el escritorio de CCA.
- **Barra de funciones.** El panel escalable en el lado izquierdo del espacio de trabajo de CCA en el cual es posible seleccionar las funciones de red a configurar y las tareas a ejecutar. Si no conoce el nombre de una función, puede buscarla. Para saber más sobre la barra de funciones, consulte **Barra de funciones, página 27**.
- **Escritorio.** El lado derecho del espacio de trabajo de CCA, en el que aparecen el Tablero, las ventanas de configuración y los asistentes. Usted ve los informes aquí e ingresa la información que configura las funciones de red. Para aprender más sobre el escritorio, consulte **Escritorio de CCA, página 29**.
- **Barra de estado.** La barra que aparece en la parte inferior de la ventana CCA. Cuando se inicia CCA, aparece la barra de estado y avanza hacia la derecha a medida que la red reconoce los dispositivos. La barra de estado también indica cuando se está cargando los datos de voz. Cuando finaliza este proceso, CCA está listo para su uso.

  Éste repite su proceso de reconocimiento para cada intervalo de encuesta de red. Si pierde conectividad con el sitio de clientes o dispositivo autónomo, la barra de estado muestra *Sin conectividad*.
- **Vista de Topología.** Un mapa de la red y mucho más, dependiendo de las opciones que seleccione en la vista. Para aprender más, consulte **Vista Topología, página 34**.

- **Vista del panel frontal.** Una lista jerárquica de los dispositivos en su red, un gráfico de la caja de cableado de los dispositivos y el estado de cada dispositivo y sus puertos. Para aprender más, consulte **Vista del panel frontal, página 44**.

Barra del menú

La barra del menú tiene funciones para ayudarle a utilizar CCA. Las funciones se agrupan en los siguientes menús: Sistema, Ventana y Ayuda.



Menú	Función	Lo que se puede hacer
Sistema	Conectar	Conexión a un sitio o dispositivo autónomo.
	Actualizar	Actualiza la Vista del panel frontal y la vista Topología al encuestar a los miembros del sitio.
	Actualizaciones de aplicación	Verifica las actualizaciones de la aplicación.
	Notificación de mensajes del sistema	Recibe notificaciones por correo electrónico de mensajes del sistema.
	Configuración de página, Vista previa, Imprimir	Utilice las opciones de impresión estándares para imprimir vistas, ventanas y gráficos.
	Preferencias	Configure las preferencias de usuario para CCA.
	Barra de funciones	Configure el modo de vista de la barra de funciones (Estándar o Autohide).
Ventana	Seleccione una ventana de la lista de ventanas abiertas	Navegue hasta una ventana en una lista de ventanas abiertas.

Menú	Función	Lo que se puede hacer
Ayuda	Contenidos	Consulte el tema de ayuda que presenta CCA.
	Novedades	Consulte una lista de las nuevas funciones y mejoramientos que se agregaron a CCA de versión a versión.
	Ayuda para la Ventana Activa	Consulte el tema de ayuda para la ventana o vista que esté activa. También se puede acceder a ayuda para la ventana actual presionando **F1**.
	Comentarios	Envíe sus comentarios sobre CCA a Cisco.
	Información de inicio	Consulte un resumen de las nuevas y modificadas funciones para la versión actual.
	Información de soporte	Consulte cómo contactar al Centro de soporte para pequeñas empresas y cómo generar un archivo de registro de solución de problemas.
	Acerca de	Consulte la información de la licencia y el identificador para la versión de CCA que está utilizando.

Barra de herramientas

La barra de herrramientas contiene iconos para las tareas que se realizan con mayor frecuencia. Esta tabla describe las acciones que toma CCA cuando usted hace clic en los iconos. Pase el ratón sobre los iconos de la barra de herramientas para mostrar una sugerencia que identifica a cada uno de ellos.

Icono	Acción
Conectar	Abre la ventana Conectar, donde se identifica un sitio de clientes o un dispositivo autónomo para que CCA los administre.
Actualizar	Actualiza la Vista del panel frontal y la vista Topología al encuestar a los miembros del sitio del cliente. CCA actualiza el estado de los dispositivos y puertos y muestra todo miembro nuevo.
Imprimir	Envía un archivo de impresión para un gráfico, informe, o selecciones de ayuda en línea hacia una impresora.
Preferencias	Abre la ventana Preferencias, donde se pueden establecer las preferencias del usuario.
Guardar configuración	Hace que los cambios realizados a la configuraciÃ³n del dispositivo sean permanentes, es decir, los cambios permanecen en efecto despuÃ©s que el dispositivo se apaga y enciende nuevamente.
Usuarios y teléfonos	Abre la ventana Usuarios y teléfonos, donde se configuran las opciones para comunicación de voz.
Servidor VPN	Abre la ventana Servidor VPN, donde se configura un servidor VPN para enviar políticas de seguridad a un dispositivo.
Firewall y DMZ	Abre la ventana Firewall y DMZ, donde se configura un firewall o se crea un DMZ.

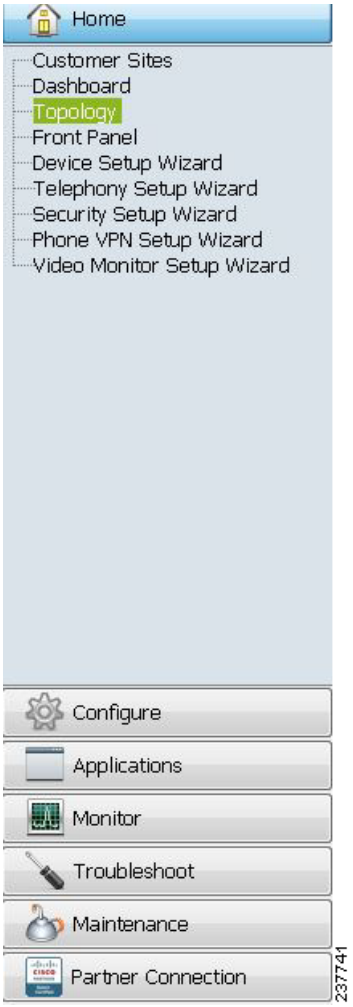
Icono	Acción
Redes inalámbricas	Abre la ventana Redes inalámbricas, donde se configuran funciones de seguridad en un controlador de WLAN y sus puntos de acceso asociados.
Smartports	Abre la ventana Smartports, donde se configuran los puertos y dispositivos al asignarles perfiles.
Configuración de puertos de switch	Abre la ventana Configuración de puertos del switch, donde es posible visualizar el estado de los puertos en un dispositivo seleccionado y modificar la configuración de los puertos.
Inventario	Abre la ventana de inventario, lo que muestra el inventario de los tipos de dispositivos en la comunidad, los números de serie, las direcciones IP, y las versiones de software o el inventario de un solo dispositivo.
Estado	Abre la ventana Estado, donde es posible monitorear cierta cantidad de mediciones de *estado* de los dispositivos para evitar las detenciones y asegurar que su red funcione eficientemente.
Notificación de eventos	Abre la ventana Notificación de eventos que describe las condiciones de la red de las que debe estar informado y podráan necesitar acciones de su parte.
Tablero	Abre la ventana Tablero, que entrega una vista gráfica del estado del sistema, incluyendo la utilización de almacenaje en la memoria flash del UC500, utilización de PoE, temperatura, eventos, correo de voz, memoria y utilización de CPU.
Topología	Abre la vista Topología, la que muestra un mapa de la red de los miembros de la comunidad y mucho más, dependiendo de las opciones de topología que se seleccionen.
Panel frontal	Abre la vista Panel frontal, la que muestra una lista jerárquica de los dispositivos de la comunidad; un gráfico de gabinete de cableado de los dispositivos, y el estado de cada dispositivo y sus puertos.
Leyenda	Abre la ayuda en línea para obtener una explicación de las convenciones gráficas usadas en CCA.

Icono	Acción
Ayuda para la ventana Activa	Abre la ayuda en línea hacia una explicación de la ventana activa. Si no hay una ventana activa, se muestra el tema *Introducción*.
Comentarios	Abre una página web donde usted puede dejar comentarios acerca de su experiencia con CCA.

También puede introducir términos a la derecha de la barra de herramientas y hacer clic en **Buscar** para buscar los términos en los temas de ayuda en línea.

Barra de funciones

La barra de funciones se ubica al costado izquierdo del escritorio de CCA.



Las funciones se agrupan en estos menús para identificar las categorías de tareas:

- **Inicio**, para abrir las vistas de Tablero, Topología y Panel frontal y ejecutar asistentes de configuración de dispositivos, telefonía, VPN de teléfonos, inalámbrica y otros.
- **Configurar**, para configurar dispositivos, puertos, enrutamiento de redes, LAN inalámbricas, y funciones de seguridad y telefonía.
- **Applicaciones**, para activar y configurar las opciones de configuración de Smart Applications o aplicaciones de terceros.
- **Monitorear,** para monitorer su red, ver informes de estado del sistema y de telefonía y especificar comandos para IOS de Cisco y para Unity Express (CUE) de Cisco.
- **Solución de problemas**, para solucionar problemas de red y de voz y crear registros que pueda utilizar el Centro de Soporte para pequeñas empresas

de Cisco para ayudar en la búsqueda y solución de problemas de redes y sistemas.

- **Mantenimiento**, para mantener su red, actualizar software, administrar licencias, cargas telefónicas y archivos en el UC500.
- **Conexión de socios**, para acceder a la comunidad de soporte de Cisco Small Business, la página de producto del UC500, alimentaciones RSS, descargas de software para UC500, VOD (video por demanda) para CCA, y al sitio central de socios en Cisco.com.

Cuando se selecciona una función en uno de estos menús aparece el contenido en una ventana separada del navegador.

Modo Standard y Modo Autohide

La barra de funciones puede configurarsr como modo standard o modo autohide:

- Cuando la barra de funciones esté en *modo estándar*, puede limitarla para aumentar el espacio para las ventanas en el escritorio de CCA. Para esto, coloque el cursor en el borde derecho de la barra de funciones y arrástrelo hacia la izquierda.
- Cuando la barra de funciones esté en *modo autohide*, sólo aparece cuando mueve el cursor hacia el borde izquierdo del espacio de trabajo de CCA. Vuelve a desaparecer cuando mueve el cursor hacia cualquier dirección en el espacio de trabajo de CCA fuera del límite de la barra de funciones.

Para configurar el modo de visualización para la barra de funciones, seleccione **Sistema** > **Barra de funciones** en la barra de menú y seleccione **Modo estándar** o **Modo Autohide**.

Escritorio de CCA

El escritorio de CCA es el punto focal de la interfaz del usuario. Es donde usted realiza estas tareas:

- Visualizar la **Tablero**, una vista gráfica del estado del sistema, incluyendo la utilización de CPU, utilización de PoE y de almacenamiento de la memoria flash del UC500, temperatura, alertas de eventos, estado de VPN y correo de voz.
- Visualizar la **Vista Topología**, un mapa de red del sitio de clientes que CCA está administrando. La vista muestra la información del nodo, información del enlace y dispositivos cercanos.

- Visualizar la **Vista del panel frontal**, una imagen de los paneles frontales de los dispositivos en la comunidad. Puede hacer clic en los dispositivos y puertos representados, y elegir las opciones de configuración desde un menú emergente.
- Visualizar asistentes de configuración. Algunos asistentes de configuración, como el Asistente de configuración de telefonía y el Asistente de conectividad SR520-T1 se inician automáticamente cuando se conecta a un dispositivo que está en estado por defecto de fábrica.
- Especifique la información para configurar las funciones de la red. Usted realiza esta tarea al usar las ventanas de funciones o pasos a modo de guía.
- Visualizar informes y gráficos. Busque las palabras Informes y Gráficos en los menús en la barra de funciones. Ellas acompañan muchas de las funciones de red ofrecidas ahí.

Iniciar una vista por defecto cuando CCA se conecta a un dispositivo es una preferencia que usted puede definir. Puede iniciar ya sea la vista, ambas vistas o ninguna. Consulte **Configuración de preferencias, página 55**.

Tablero

La vista Tablero necesita la Versión 10.0.0.0 ó posterior de Adobe Flash Player y Microsoft Internet Explorer instaladas en la PC que ejecuta CCA. Javascript debe estar activado para el navegador Microsoft Internet Explorer.

Visión general

El Tablero aparece en la ventana principal cuando se conecta inicialmente a un dispositivo o sitio de cliente con CCA. Entrega una vista intuitiva, gráfica y de fácil visualización del estado del sistema para los dispositivos de la serie 500 de Unified Communications de Cisco y para otros dispositivos administrados.

Si se cierra la ventana Tablero, siempre se puede volver a abrirlo si se navega hasta **Inicio** > **Tablero**.

Se puede especificar si el Tablero se muestra automáticamente cuando se conecta a la red. Para acceder a esta configuración, navegue hasta **Sistema** > **Preferencias**, haga clic en la ficha General y marque o desmarque la opción **Mostrar tablero cuando esté conectado a la red**.

Uso de Tablero

La interfaz del usuario del Tablero consiste en una serie de ventanas y una paleta desde la que se puede arrastrar y soltar ventanas en el área de visualización principal.

- Haga clic en **Mostrar paleta** para ver la paleta. Por defecto, se encuentra oculta.
- Utilice los botones de flecha hacia la derecha y hacia la izquierda para avanzar por las ventanas disponibles.
- Arrastre y suelte o haga doble clic en los iconos de la paleta para ubicar ventanas en el área de visualización.
- Ubique el ratón sobre los elementos de la vista gráfica para ver las sugerencias de herramientas con valores numéricos o porcentuales.

Cada elemento de la ventana Tablero entrega controles para:

- Minimizar y maximizar la ventana en la vista
- Seleccionar un dispositivo diferente para ver, si es aplicable
- Modo de navegación de presentación de diapositivas, con controles de pausa y reproducción

  En el modo Presentación de diapositivas, la pantalla se actualiza para mostrar información sobre estados momentáneos para cada dispositivo a los intervalos de navegación especificados. Si sólo existe un dispositivo, seleccionar el modo Presentación de diapositivas no tiene efectos en la pantalla.
- Cerrar la ventana y moverla de vuelta a la paleta.
- Configurar ventanas

  Por ejemplo, la ventana Temperatura del tablero puede configurarse para mostrar la temperatura en grados Celsius o Fahrenheit. Pueden configurarse intervalos de actualización de datos y de navegación de presentación de diapositivas para todas las ventanas.

Para acceder a la configuración para las ventanas del tablero, haga clic en el icono de configuración en la barra de la ventana.

Los cambios a la vista Tablero se guardan en todas las sesiones.

Pantallas disponibles de estado del sistema

La tabla a continuación muestra y describe las ventanas disponibles de estado del sistema.

Ventana	Descripción
Estado del sistema	Muestra información general para el dispositivo seleccionado: ▪ Nombre de host y tipo de dispositivo ▪ Dirección IP de WAN, máscara de subred y del gateway ▪ Direcciones IP del servidor DNS ▪ Versión de IOS de Cisco ▪ Tiempo de actividad ▪ Fecha de última actualización
Uso de la CPU	Porcentaje de la capacidad de la CPU que se está utilizando en los últimos 5 segundos, en el último minuto y en los últimos 5 minutos para el dispositivo seleccionado.
Utilización de PoE	Porcentaje disponible y porcentaje utilizado de energía para puertos PoE del dispositivo. Ubique el ratón sobre el gráfico para ver el consumo de energía en Watts. **NOTA** Utilización de PoE no se muestra en la actualidad para los switches de la serie ESW500 con PoE.
Uso de flash	Porcentaje disponible y porcentaje utilizado de almacenamiento para la memoria flash del dispositivo seleccionado. Ubique el ratón sobre el gráfico para ver la utilización de almacenamiento en Mbytes.
Uso de la memoria	Porcentaje disponible y porcentaje utilizado de capacidad de memoria del dispositivo seleccionado. Ubique el ratón sobre el gráfico para ver la asignación de memoria en Mbytes.

Ventana	Descripción
Eventos	Tipo y descripción para los mensajes recientes de alerta de notificiación de eventos. Para mayores detalles, navegue hata **Monitorea** > **Notificación de eventos**. También se puede ubicar el ratón sobre el evento para ver una sugerencia de herramienta con la descripción extendida y acciones recomendadas.
Temperatura	Para los dispositivos, se puede medir la temperatura precisa, en grados Celsius o Fahrenheit.
Estado de correo de voz	Muestra la información y estado de almacenamiento de correo de voz por buzón y para todo el sistema, incluyendo: ▪ Versión de Unity Express (CUE) de Cisco ▪ Porcentaje (%) utilizado en todo el sistema ▪ Información por buzón - ID de usuario/nombre de grupo de búsqueda asociado con el buzón - Anexo - Tipo—Personal o GDM (Buzón de entrega general) - Tamaño—Cantidad de almacenamiento asignado, en minutos
Estado de la red VPN	Si está configurada EZVPN, se muestra la dirección IP pública, la dirección IP de VPN y el estado actual: Activa; Activa - Detenida, Activa sin IKE, Negociando o Desactivada. El estado de VPN también puede verse si se navega hasta **Monitorear** > **Seguridad** > **Estado VPN**.

Ventana	Descripción
Cliente inalámbrico (AP541N)	Para una rápida visión del estado de clientes inalámbricos, seleccione **Inicio** > **Tablero** para mostrar el tablero del sistema, luego, arrastre y suelte el elemento Cliente inalámbrico desde la paleta hacia el área principal del tablero. El elemento Cliente inalámbrico del tablero muestra la dirección MAC, la dirección IP, el SSID, el tipo de seguridad y el tipo de dispositivo para los clientes inalámbricos asociados para los puntos de acceso AP541N. En el tablero no se muestra n ni el estado del controlador de LAN inalámbrica ni el estado del AP521.

Vista Topología

Esta vista aparece cuando se realiza una de estas acciones:

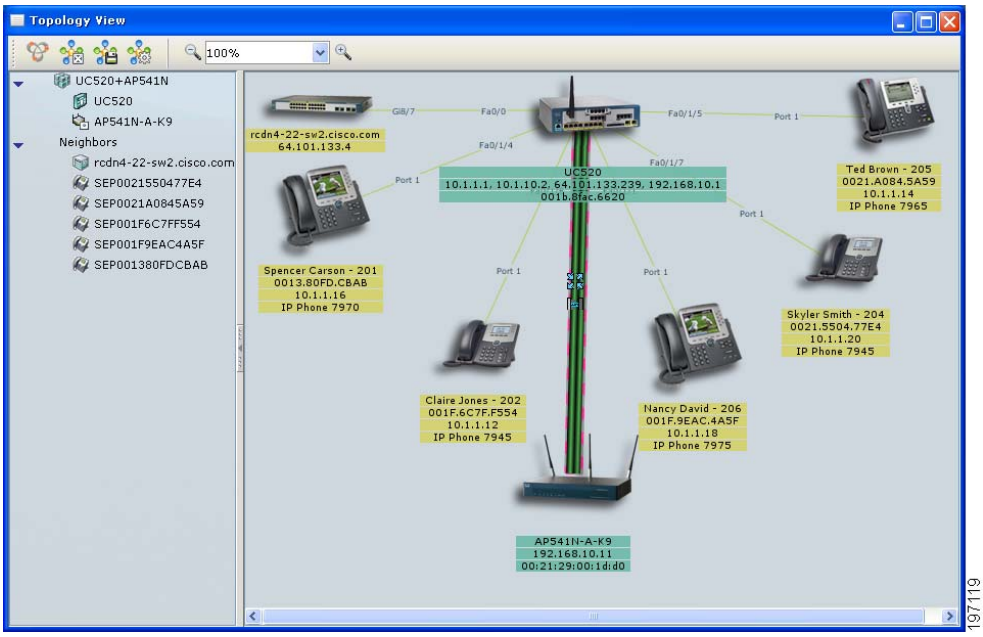
- Conectar CCA los dispositivos que desea administrar.
- Seleccionar **Inicio** > **Topología** en la barra de funciones.
- Haga clic en el icono Vista Topología de la barra de herramientas.

Visión general

Utilice esta vista para visualizar la topología de los dispositivos que gestiona y sus conexiones. Utilice sus partes; la **Barra de herramientas**, la **Trama izquierda — Dispositivos miembros del sitio y cercanos** y la **Trama derecha — Mapa de topología** para realizar **Tareas** que manipulen la vista, la guarden y le entreguen información acerca de los dispositivos de ella.

NOTA Los softphones Cisco IP Communicator (CIPC) no se muestran en la vista Topología porque no hay información de Protocolo de descubrimiento de Cisco (CDP) para los softphones.

Haga clic con el botón derecjho en los iconos de la vista Topología para las opciones de localización para agregar o eliminar un dispositivo del sitio de clientes, abrir la utilidad de configuración de dispositivos nativos o realizar otras tareas de administración. Consulte **Tareas, página 38**.



Barra de herramientas

La Vista de topología tiene su propia barra de herramientas. Esta tabla describe las acciones que realiza CCA cuando usted utiliza las opciones de la barra de herramientas.

Opción	Cómo utilizarla
Descubrir dispositivos Bonjour	Haga clic para descubrir las cámaras de vídeo PVC2300 y WVC2300 de Cisco y las impresoras de terceros con soporte de Bonjour. Haga clic con el botón derecho en un dispositivo Bonjour y seleccione la opción Utilidad de configuración para administrar estos dispositivos usando sus herramientas de administración web incorporadas.
Diseño automático	Haga clic para redistribuir el espacio e información en la vista.
Guardar Layout	Haga clic en ello para guardar las ubicaciones de los dispositivos en el mapa de la topología.

Opción	Cómo utilizarla
Opciones de topología	Haga clic en ello para iniciar la ventana Opciones de topología, en la cual usted controla la información que aparece en la vista. Por ejemplo, se puede controlar cuánta información se muestra acerca de los enlaces y nodos utilizando las casillas de la ficha **Mostrar información**. Consulte **Opciones de topología, página 42**.
Controles de zoom	Cada vez que se inicia una vista, la trama derecha aparece con un 100% de magnificación. Para alejarse: ▪ Haga clic o mantenga presionada la tecla "-" el icono de lupa, o ▪ Pulse el botón "-" en el teclado, o ▪ Seleccione una magnificación menor en la lista desplegable, o ▪ Especifique un número menor que 100 en el campo de texto. Para acercarse de nuevo, use uno de los siguientes métodos: ▪ Haga clic o mantenga pulsado el icono de lupa "+". ▪ Pulse el botón "+" en el teclado. ▪ Seleccione una magnificación mayor en la lista desplegable. ▪ Especifique un número mayor, hasta 100, en el campo de texto.

Usted puede seleccionar cualquiera de las primeras acciones desde el menú que aparece cuando usted hace clic con el botón secundario en cualquier lugar del fondo de la trama derecha.

Trama izquierda — Dispositivos miembros del sitio y cercanos

La trama izquierda es un *diagrama de árbol*. Muestra una lista expandida con el nombre del sitio de clientes y cada miembro del sitio. También existe una lista de los dispositivos cercanos de los miembros del sitio.

Para un dispositivo autónomo, la lista muestra sólo ese dispositivo y sus cercanos.

Si no se utiliza un ratón, debe usarse la tecla **Tab** para seleccionar el árbol, y luego, utilizar las teclas de flechas hacia arriba y abajo para desplazarse dentro de éste.

Cuando se selecciona un dispositivo en la vista de árbol, el dispositivo correspondiente se selecciona en la trama derecha, y ésta avanza automáticamente hasta que sea visible dicho dispositivo.

Estado del dispositivo

El árbol muestra el estado de los dispositivos con los siguientes colores:

Color	Estado
 Rojo	Apagado o no conectado
 Verde	Conectado y funcionando
 Azul	Desconocido

Utilización de la ventana emergente

Si se hace clic con el botón secundario sobre un dispositivo, o si se presiona **Shift-F10**, en la trama izquierda se abre una ventana emergente. Su menú es una lista de tareas, por ejemplo, ver las propiedades, cambiar el nombre de host, el reinicio de un dispositivo, o ver una gráfica del ancho de banda—que se pueden realizar con el dispositivo. Se trata de la misma ventana emergente que se abre cuando se hace clic con el botón secundario en un dispositivo de la trama derecha.

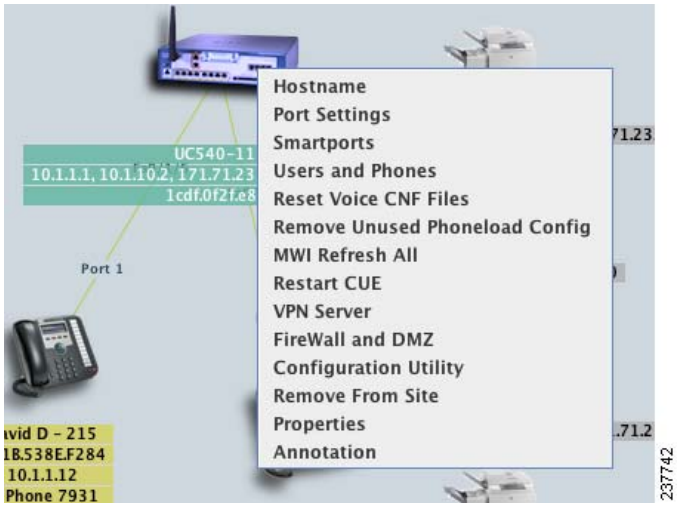
Trama derecha — Mapa de topología

La trama derecha es el *mapa de topología*. Muestra los enlaces entre los dispositivos y entrega información de ellos. Las normas que se aplican a ella son las mismas que para la trama izquierda:

- Sus contenidos dependen de si se está administrando un sitio de clientes de CCA con múltiples dispositivos o un dispositivo autónomo y si se le ha solicitado ver los dispositivos cercanos en la ventana Opciones de topología.

- Haga clic en un icono de dispositivo en la vista Topología para abrir ventanas para realizar tareas con el dispositivo seleccionado. También es posible realizar tareas, independientes de los dispositivos, que manipulen la vista de esta trama,

  Por ejemplo, el siguiente menú se muestra cuando se hace clic con el botón derecho en el UC500 de la vista Topología.



- El estado del dispositivo se indica con los mismos colores.

Tareas

Esta tabla indica las tareas que se pueden realizar desde esta vista e indica cómo realizarlas.

Tarea	Cómo realizarla
Reordenar el diseño	Para hacer que dispositivos, enlaces e información sean más visibles en esta vista: ▪ Arrastrar dispositivos a lugares que usted prefiera. ▪ *Unir* dispositivos que usted desea mover como un grupo; es decir, mantener presionado un botón del mouse y dibujar un rectángulo alrededor. Cuando se arrastra un dispositivo, se les arrastra a todos.

Tarea	Cómo realizarla
Mostrar información del dispositivo y el enlace	Para mostrar las propiedades de un dispositivo o enlace, haga clic con el botón secundario o doble clic sobre él y seleccione **Propiedades** del menú emergente. Las propiedades de un dispositivo son su nombre, tipo, dirección IP, dirección MAC y la versión de IOS de Cisco que se ejecuta. Las propiedades de un enlace son las identidades de los puertos conectados y el estado del enlace. Para monitorear el ancho de banda que utiliza un dispositivo, haga clic con el botón secundario o doble clic sobre él y seleccione **Gráficos de ancho de banda** del menú emergente. Para monitorear el uso de un enlace, haga clic con el botón secundario o doble clic sobre él y seleccione **Gráficos de enlace** del menú emergente.
Mostrar VLAN	Si está administrando múltiples dispositivos como parte de un sitio de clientes, se pueden mostrar los enlaces a VLAN en el mapa de topología. Haga clic en el icono de opciones para abrir la ventana Opciones de topología y utilice la ficha **Mostrar VLAN** .
Cómo agregar dispositivos a un sitio de clientes	Para agregar un miembro a sitio de clientes, haga clic con el botón secundario o doble clic en cualquier candidato y seleccione **Agregar al sitio** desde el menú emergente.
Eliminación de dispositivos desde un sitio de clientes	Para eliminar un miembro de un sitio de clientes, haga clic con el botón secundario en cualquier dispositivo y seleccione **Eliminar del sitio** en el menú emergente.
Actualizar la vista	Cuando se activa la función de encuesta de red, CCA periódicamente encuesta los dispositivos gestionados y actualiza la topología de red cuando se elimina o se agrega un dispositivo. Si sabe que ha ocurrido un cambio y usted desea ver el cambio entre intervalos de encuesta, haga clic en el icono de la vista **Actualizar** en la barra de herramientas. **NOTA** Para activar o desactivar la función de encuesta de la red y se cambia el intervalo de encuesta, use la ventana Preferencias. Consulte **Configuración de preferencias, página 55**.

Tarea	Cómo realizarla
Restablecimiento de los archivos de configuración de voz (CNF)	Seleccione **Restablecer archivos CNF de voz** para hacer que CCA regenere los archivos de configuración del eXtensible Markup Language (XML) para los teléfonos IP para que puedan actualizar y reconocer nuevas configuraciones. Esto puede ser necesario luego de cambiar los archivos de localización de teléfonos.
Eliminación de configuraciones de voz sin usar	Seleccione **Eliminar configuraciones de voz sin usar** para eliminar la CLI de carga de teléfonos que no se use en la configuración.
Actualización de las MWI en todos los teléfonos	Seleccione **Actualizar MWI en todos**para actualizar el Indicaro de mensaje en espera (MWI) en todos los teléfonos para reflejar el estado actual de los buzones de correo de voz.
Cambiar nombre de host	Haga clic con el botón secundario en el dispositivo, seleccione **Nombre de host** en la ventana emergente, y utilice la ventana Nombre de host.
Comentar objetos y enlaces	Se puede agregar un campo de texto, que se denomina como *comentario* bajo las nubes de dispositivos y redes y en los puntos extremos de los enlaces. Un comentario es útil para mostrar información descriptiva que, de otra forma, no aparece en el mapa de topología. Cuando se agregar una nube de redes o enlaces, se abre la ventana Comentario. Para comentar un dispositivo que ya esté en el mapa, haga clic con el botón derecho, seleccione **Comentario** en la ventana emergente y utilice la ventana Comentario. Consulte **Comentarios, página 44**. Si desea ocultar las anotaciones en la Vista de topología, abra la ventana Opciones de topología y desmarque **Anotaciones** en la ficha **Mostrar información** .

Tarea	Cómo realizarla
Actualizar el software	Arrastre y suelte un archivo de imagen de software desde su PC hasta el icono de un dispositivo. (El dispositivo debe ser miembro del sitio de clientes.) El archivo puede estar en una unidad asignada o una unidad de red, como también en una unidad local. Para actualizar el software en más de un dispositivo a la vez, utilice la ventana Actualización de software.
Descubrir dispositivos Bonjour	Haga clic en el icono Bonjour de la barra Topología o haga clic con el botón derecho en el fondo de la vista Topología y seleccione**Descubrir dispositivos Bonjour** para descubrir cámaras de vídeo PVC2300 y WVC2300 de Cisco e impresoras de terceros con soporte Bonjour. Seleccione la opción de Utilidad de configuración para administrar estos dispositivos usando sus herramientas de administración web incorporadas.
Agregar una nube de redes	Haga clic con el botón derecho en el fondo del mapa de topología, y seleccione **Agregar nube de redes** de la ventana emergente. Asigne una etiqueta a la nube en la ventana Comentario que aparece y arrástrela a cualquier área del mapa que desee. Se puede cambiar la etiqueta o eliminar la nube haciendo clic con el botón derecho y seleccionando una acción del menú.
Agregar un enlace	Se puede agregar manualmente un enlace al mapa. Apunte al nodo desde el que desee hacer el enlace, presione **Ctrl** y haga clic, apunte al nodo al que desea conectar el enlace y presione **Ctrl** y haga clic de nuevo. Luego, haga clic con el botón derecho en cualquiera de los nodos y seleccione **Agregar enlace** en la ventana emergente, Se dibuja un enlace entre los nodos y aparece la ventana Comentario. En sus campos, especifique etiquetas para los puntos extremos del enlace.

Opciones de topología

Esta ventana aparece cuando se selecciona el icono Opciones de topología en la barra de herramientas de la vista Topología. Utilice la ventana para especificar lo que desea ver en la Vista de topología.

Cualquier dispositivo que ejecuta el Protocolo de descubrimiento de Cisco (CDP) aparecerá en la vista de topología. No todos estos dispositivos pueden administrarse con Configuration Assistant.

CCA tiene la capacidad de iniciar en forma cruzada el administrador de dispositivos nativo o utilidad de configuración para ciertos dispositivos, tales como los routers seguros de la serie SA500 y los switches de la serie ESW500. Para iniciar el administrador de dispositivos nativo, haga clic con el botón derecho en el dispositivo de la vista Topología y seleccione **Utilidad de configuración** del menú de la lista desplegable.

La ventana tiene estas fichas:

- **Mostrar dispositivos cercanos**, para seleccionar los dispositivos cercanos que usted desea ver
- **Mostrar información**, para seleccionar la información acerca de enlaces y nodos que desea ver
- **Mostrar VLAN**, para mostrar los enlaces VLAN de la comunidad y para seleccionar los colores que los representan

Cuando termine con esta ventana, haga clic en **Aceptar**.

Mostrar dispositivos cercanos

Estas casillas de verificación controlan los vecinos que se pueden ver:

- **Teléfonos IP**: Teléfonos con funciones completas que proporcionan comunicación de voz en una red IP.
- **Otros dispositivos cercanos**: márquela para ver dispositivos cercanos que detecta el Protocolo de descubrimiento de Cisco (CDP); por ejemplo, puntos de acceso y dispositivos que CCA no admite como miembros de la comunidad.

Mostrar información

Estas casillas de verificación controlan la información que se muestra para los enlaces y nodos del mapa de topología:

- **ID de interfaz**; márquela para ver las ID de las interfaces a las que están conectados los enlaces.
- **Velocidad real** si desea ver la información de velocidad del enlace, en oposición a la velocidad administrativa de un enlace.
- **Nombre de host** para ver los nombres de host de los nodos.
- **Dirección IP** para ver las direcciones IP de los nodos.
- **Dirección IP** para ver las direcciones MAC de los nodos.
- **Comentarios** para ver los comentarios de enlaces y nodos.

Mostrar VLAN

Siga los siguientes pasos para mostrar los enlaces VLAN en el mapa de topología:

PASO 1 En la carpeta VLAN, haga clic en **Asignar color** para las VLAN cuyos enlaces usted desea destacar.

PASO 2 En la ventana Selección de color, haga clic en el color para destacar que desea utilizar y haga clic en **Aceptar**. El número de VLAN se mueve sobre la carpeta VLAN a la lista de VLAN que tienen un color para destacar. El botón **Asignar color** se transforma en el botón **Modificar color** y muestra el color que se seleccionó.

PASO 3 Marque la casilla al lado del número de VLAN para activar el color para destacar en la Vista de topología. Si usted desmarca posteriormente la casilla, se desactiva el destacado.

Notas:

- Para cambiar el color para destacar de una VLAN, haga clic en su botón **Modificar color** y seleccione un color diferente en la ventana Selección de color.
- Para eliminar el destacado de una VLAN, haga clic en su botón **Eliminar color**. Los botones **Modificar color** y **Eliminar** de VLAN desaparecen y el número de VLAN vuelve a la carpeta VLAN con su botón **Asignar color**.

Comentarios

Esta ventana aparece cuando usted:

- Hace clic con el botón derecho en el mapa de topología y selecciona Comentarios en el menú emergente.
- Agrega una nube de redes
- Agrega un enlace entre nodos en el mapa de topología; por ejemplo, entre un dispositivo y una nube de redes o entre dispositivos.

La información aparece bajo el icono del nodo. Si se está comentando un enlace, especifique información de identificación para cada uno de los puntos extremos del enlace. Haga clic en **Aceptar** cuando termine.

Se puede ocultar los comentarios en el mapa de topología al desmarcar Comentarios en la ficha Mostrar información de la ventana Opciones de topología.

Vista del panel frontal

Esta vista aparece cuando se realiza una de estas acciones:

- Especificar en la ventana Preferencias que usted desea que la Vista del panel frontal se abra cuando se conecte CCA. Consulte **Configuración de preferencias, página 55**.
- Seleccionar **Inicio** > **Panel frontal** en la barra de funciones.
- Hacer clic en el icono Vista Topología de la barra de herramientas.

La vista tiene dos partes interrelacionadas: la **Trama izquierda** y la **Trama derecha**. Utilícelas para **Seleccionar dispositivos** y **Selección de puertos** para que se pueda verificar y cambiar configuración. También puede **Cambiar de posición los dispositivos** en la vista. Para ver el efecto de los cambios, se puede **Actualización de la vista**.

Trama izquierda

La trama izquierda es un diagrama de árbol que muestra los dispositivos miembros marcados bajo un nombre de sitio de clientes. Cada nombre de dispositivo tiene un cuadro a su lado. Marque el cuadro para visualizar el panel frontal del dispositivo en la trama derecha.

No todos los dispositivos tienen una vista de panel frontal. Además, los dispositivos desconocidos no muestran una vista de panel frontal.

El diagrama de árbol muestra el estado de los dispositivos con los siguientes colores:

- **Verde**. El dispositivo está conectado y funcionando.
- **Amarillo**. Se detectó una condición de fallo. Ubique el puntero del ratón sobre el icono del dispositivo para visualizar el mensaje de la condición de fallo.
- **Rojo**. El dispositivo está inactivo o no está conectado.

Trama derecha

La trama derecha muestra lla vista de panel frontal para los dispositivos que se seleccionan en la trama izquierda. Se visualizarán sus puertos y ranuras de módulos igual que en un armario de cableado.

Seleccionar dispositivos

Es posible seleccionar un dispositivo de dos maneras:

- Haga clic en su panel frontal.
- Seleccione el icono del dispositivo en el diagrama de árbol.

Cuando se hace clic en un dispositivo, aparece un rectángulo amarillo a su alrededor, indicando que está seleccionado. Para seleccionar múltiples dispositivos, mantenga presionada la tecla **Ctrl,** y haga clic en los dispositivos que desee. Para anular la selección de un dispositivo, mantenga presionada la tecla **Ctrl**, y haga clic en el dispositivo cuya selección desee anular.

Es posible seleccionar un grupo de dispositivos y, luego, hacer clic con el botón derecho en un dispositivo para visualizar un menú emergente. Utilice el menú emergente para verificar o cambiar la configuración del dispositivo. Las opciones del menú emergente sólo se aplican a los dispositivos seleccionados. También es posible utilizar las opciones de la barra de funciones para verificar o cambiar la configuración del dispositivo. Si no es aplicable una opción de la barra de funciones a los dispositivos seleccionados, dicha selección se ignora.

Selección de puertos

Esta tabla muestra las opciones para seleccionar puertos.

NOTA No pueden seleccionarse los puertos de un controlador de WLAN.

Si se desea...	Entonces...
Seleccionar un solo puerto	Haga clic en el puerto. Aparece un menú si se hace clic con el botón derecho.
Seleccionar todos los puertos de un dispositivo	Haga clic en cualquier puerto y seleccione **Seleccionar todos los puertos** en el menú emergente.
Seleccionar múltiples puertos en el mismo dispositivo o en varios diferentes.	Utilice cualquiera de los siguientes métodos: ▪ Mantenga presionada la tecla **Ctrl**, y haga clic en los puertos que desee seleccionar. ▪ *Encierre* los puertos que desee seleccionar; es decir, mantenga presionado un botón del ratón y arrastre un rectángulo alrededor del grupo de puertos. Si también se mantiene prsionada la tecla **Ctrl**, se puede agregar grupos de puertos no adyacentes a la selección.

Para anular la selección de un puerto, mantenga presionada la tecla **Ctrl** y haga clic en el dispositivo cuya selección desee anular.

Cuando se hace clic con el botón derecho para seleccionar un solo puerto, aparece un menú emergente. Para visualizar un menú emergente cuando se seleccione más de un puerto, se debe hacer clic en uno de los puertos. Utilice el menÃº emergente para verificar o cambiar la configuraciÃ³n del puerto. Los elementos del menÃº emergente sÃ³lo se aplican a los dispositivos seleccionados. También es posible utilizar los elementos de la barra de funciones para verificar o cambiar la configuración del puerto. Si no es aplicable un elemento de la barra de funciones a los puertos seleccionados, dicha selecciÃ³n se ignora.

Cambiar de posición los dispositivos

Es posible cambiar el orden de los dispositivos para que reflejen su ubicación física en su armario de cableado. Para reubicar un dispositivo, arrastre su icono en el diagrama de árbol hasta una nueva posición.

Actualización de la vista

Para actualizar la vista Panel frontal, haga clic en el icono Actualizar en la barra de herramientas. Esta acción es útil si se sabe que se ha producido un cambio en el sitio y desea visualizarlo de inmediato.

Iconos y gráficos de estado de enlaces

Esta sección explica los gráficos y colores que aparecen en la vista Topología, en la Vista del panel frontal y en las ventanas de configuración. Las explicaciones se dividen en estas categorías:

- **Iconos del dispositivo**
- **Icono de estado de dispositivo y colores de etiquetas**
- **Tipos de puertos**
- **Tipos de enlace**
- **Estado del enlace**

Iconos del dispositivo

Estos iconos de dispositivos comúnmente aparecen en las vistas y ventanas de CCA.

- El icono del dispositivo es de color rojo cuando el icono está inactivo.
- Aparece un icono del dispositivo Desconocido cuando CCA no admite un dispositivo o no admite la versión IOS de Cisco que el dispositivo está ejecutando.

Icono	Dispositivo	Icono	Dispositivo
	Sitio de cliente		Router de acceso Serie 800
	Plataforma Unified Communications Serie 500		Teléfono IP
	Switch (serie ESW500 ó Catalyst Express CE520)		Controlador LAN inalámbrico
	Punto de acceso autónomo		Punto de acceso liviano

También se podría ver estos iconos en el mapa de topología:

Icono	Dispositivo	Icono	Dispositivo
	Pila		Switch modular
	Switch de capa 3		Switch LRE
	Desconocido		Nube de redes

Icono de estado de dispositivo y colores de etiquetas

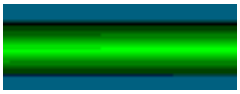
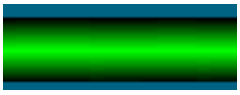
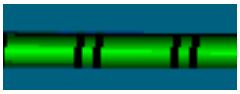
Color del icono	Activo	Inactivo	Desconocido
Color de la etiqueta	Miembro o dispositivo autónomo	Candidatos	Dispositivo periférico

Tipos de puertos

 RJ-45	 RJ-45	 RJ-11
 Mó³dulo pequeño (vacío) del small form-factor pluggable (SFP)		
 Módulo de fibra óptica SFP (LX, SX, ZX, CWDM, 100BASE-FX)		

Tipos de enlace

NOTA Las dos cañerías representan dos o más enlaces. Si una cañería es de color gris y la otra es de color verde, uno o más enlaces están bloqueados y uno o más están activos.

Tipo de icono/enlace		Tipo de icono/enlace	
	10 Mbit (bloqueado)		Gigastack
	100 Mbit		Enlace
	1 Gbit		Enrutado
	10 Gbit		Periférico
	Etherchannel		Enlaces múltiples
	Enlace agregado manualmente		

Estado del enlace

Color del enlace		Activo		Bloqueado

Aplicar y guardar la configuración

Aparece la ventana Guardar configuración cuando se sale de CCA o se selecciona **Configurar** > **Guardar configuración** en la barra de funciones.

Visión general

Cuando un dispositivo de red está en ejecución, posee dos conjuntos de configuraciones. Una es la configuración de inicio, que se almacena en la memoria flash. La otra es su configuración en ejecución, que se almacena en RAM. El dispositivo utiliza la configuración en ejecución para determinar su comportamiento.

- Cuando se hace clic en **Aceptar** o en **Aplicar** en una ventana de configuración, se hacen cambios a la configuración en ejecución. Estos cambios entran en vigor en forma inmediata.
- Cuando se selecciona **Configurar** > **Guardar configuración** o se hace clic en **Aceptar** cuando se solicita guardar la configuración al salir, se están guardando los cambios en la configuración de inicio para los dispositivos seleccionados. Ello asegura que los cambios se conservan si el dispositivo se reinicia.

Puede utilizar CCA para guardar la configuración en ejecución como la configuración de inicio, que hace permanente cualquier cambio que usted haga a la configuración en ejecución.

Guardar la configuración en ejecución no guarda los cambios que usted hace en la vista Topología. Para guardar la configuración en la vista Topología, vaya a **Inicio** > **Topología** y seleccione **Guardar diseño** en la barra de herramientas de la vista Topología.

Procedimientos

- Para guardar la configuración en ejecución de un dispositivo administrado a su configuración de inicio, seleccione el dispositivo de la lista Nombre de host y haga clic en **Guardar**.
- Para guardar las configuraciones en ejecución de todos los dispositivos administrados, seleccione **Todos los dispositivos** y haga clic en **Guardar**.

Visualización y administración de errores

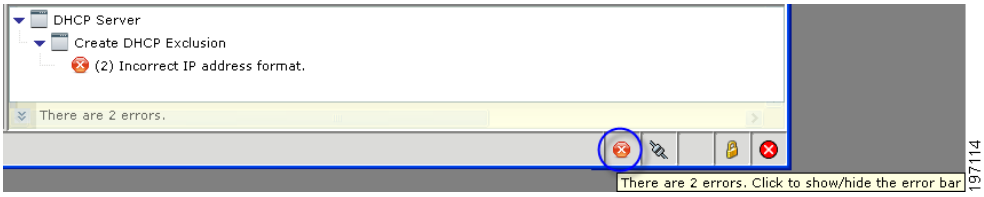
CCA le permite saber cuándo ingresa información válida poniendo un borde verde alrededor de ella.

- Cualquier cambio en la información aparece en la barra de estado.
- Cuando se aplica un cambio, el borde verde desaparece.

Administración de errores

Si se especifica información inválida al configurar los campos en CCA:

- Se verá un borde rojo alrededor de los campos que contienen errores.
- En la ventana con fichas, el número de errores en cada ficha se muestra en el encabezado de la ficha de color rojo.
- La barra de administración de erroes aparece automáticamente en la parte inferior de la ventana.



La barra de administración de errores proporciona una ubicación central para ver y administrar errores a medida que se especifican y aplican configuraciones en CCA.

Se indican todos los errores actuales en las ventanas abiertas, junto con el nombre de la ventana, el diálogo asociado (si el error aparece en un diálogo emergente) y los detalles del mensaje de error asociados. El número total de erroes en todas las ventanas abiertas se muestra en la parte inferior de la barra de administración de errores.

A medida que se resuelven errores, la barra de administración de errores se actualiza para indicar que se ha resuelto el error. Cuando se resuelven todos los errores, se cierra automáticamente.

Al trabajar con la barra de administración de errores:

- Haga clic en los botones de flecha en la jerarquía de la ventana para navegar la lista de errores en cada ventana.

- Haga clic en un mensaje de error para para poner la ventana asociada en foco y destaque el campo con el error.
- Para cambiar el tamaño de la barra de administración de errores, haga clic en el botón izquierdo en el borde superior de la barra y arrástrela.
- Para mostrar u ocultar la barra de administración de errores, haga clic en el icono del error en la parte inferior de la ventana.

Si está activada la Vista posterior de CLI (consulte la ficha Avanzadas en el diálogo Preferencias), los comandos de configuración enviados al UC500 ó al SR500 se muestran en la ventana emergente. Consulte **Configuración de preferencias, página 55**.

Mensajes de voz de advertencia

Se muestra la ventana Mensajes de voz de advertencia cuando se intenta acceder o configurar funciones de voz, pero su sistema no cumple con uno o más condiciones exigidas.

Antes de continuar, asegúrese que se cumplan las siguientes condiciones.

Mensaje de advertencia	Acciones necesarias	Función o ventana relacionada
Restablecer el sistema a la configuración por defecto de fábrica	Para ejecutar el Asistente de configuración de telefonía, primero se debe restablecer el UC500 a la configuración por defecto de fábrica. Este proceso puede tardar hasta 20 minutos. Para restablecer el UC500 a la configuración por defecto de fábrica: 1. Desde la barra de funciones a la izquierda, seleccione **Mantenimiento** >**Reiniciar/Restablecer**. 2. En la ventana Reiniciar/Restablecer, seleccione el UC500 de Cisco, marque la opción **Restablecer a configuración por defecto de fábrica** y haga clic en **Aceptar**. 3. Cuando se complete el restablecimiento, vuelva a iniciar el Asistente de configuración de telefonía.	Asistente de configuración de telefonía

Mensaje de advertencia	Acciones necesarias	Función o ventana relacionada
Asegúrese que su PC esté directamente conectada a un puerto de LAN del UC500	Para ejecutar el Asistente de configuración de telefonía, la PC que ejecuta CCA debe estar conectada directamente a un puerto LAN en el UC500 y debe obtener una dirección IP del UC500 utilizando DHCP.	Asistente de configuración de telefonía

Mensaje de advertencia	Acciones necesarias	Función o ventana relacionada
Desactive cualquier servicio TFTP de terceros que se ejecute en su PC	Si la función que se está tratando de acceder necesita que CCA utilice el servicio TFTP o FTP para transferir archivo hacia o desde el UC500, primero se debe desactivar cualquier servicio TFTP o FTP de terceros que se ejecute en su PC antes de continuar. Si se está utilizando una PC basada en Windows, se puede utilizar el Administrador de tareas de Windows para ubicar estas aplicaciones y cerrarlas. Sin embargo, estos servicios podrían no mostrarse en la ficha Aplicaciones del Administrador de tareas. También se puede abrir una ventana de comandos en su PC y dar el comando `netstat` para ver si estos servicios se están ejecutando e identificarlos por su nombres ejecutables e ID de proceso. Por ejemplo: c:\ **netstat -a -b** Una vez que se ubica el proceso TFTP o FTP de terceros, se puede ir a la ficha Procesos del Administrador de tareas de Windows y apagarlo manualmente al destacar el proceso de la lista y seleccionar **Finalizar tarea**. Para obtener mayor información, consulte la documentación de su sistema operativo, aplicación TFTP o FTP. Si no hay servicios TFTP de terceros ejecutándose, verifique la configuración de seguridad de la red y del firewall en su PC para asegurarse que se permite el tráfico TFTP entre la PC y el UC500 o intente reiniciar su PC para liberar puertos TFTP desde una sesión anterior de CCA.	Arrastre y suelte los archivos desde la PC hasta la vista Topología (imágenes de IOS de Cisco, archivos MoH, comandos de ACD básica, comandos de Contestadora automática. Asistente de configuración de telefonía Configurar > Telefonía > Gestión de llamadas > Contestadora automática Configurar > Telefonía > Gestión de llamadas > ACD básico Configurar > Telefonía > Usuarios y anexos > Discado rápido del sistema Mantenimiento > Archivo de configuración Mantenimiento > Actualización de software Mantenimiento > Administración de licencias Mantenimiento > Reiniciar/Restablecer (sólo opción Restablecer a valores por defecto de fábrica)

Configuración de preferencias

Para configurar las preferencias para CCA:

- Seleccione **Sistema** > **Preferencias** en la barra de menú.
- Haga clic en el icono Preferencias de la barra de herramientas.

Visión general

Puede personalizar gran parte de lo que hace CCA. Por ejemplo:

- Seleccionar si desea mostrar las ventanas de las vistas Topología, Panel frontal o Tablero cuando se conecte a su red usando CCA.
- Activar o desactivoar la encuesta de red y especificar con qué frecuencia CCA encuesta los dispositivos que gestiona para entregar información actualizada.
- Especificar con qué frecuencia se verifica Cisco.com en búsqueda de una nueva versión de CCA.
- Seleccionar si desea utilizar un servidor de proxy para descargar actualizaciones de CCA desde Cisco.com.
- Especificar la ubicación para archivar las configuraciones guardadas en los dispositivos que usted administra.
- Especificar opciones para el monitoreo del estado del sistema.
- Activar o desactivar la visualización de los comandos IOS de Cisco enviados al router para los cambios de configuración de telefonía (ventana Vista posterior de CLI).
- Seleccionar si se reproduce o no el archivo Cisco.wav al inicio.
- Seleccionar la imagen de fondo del escritorio.
- Activar o desactivar la recolección y carga de la actividad de utilización de CCA a Cisco.
- Activar o desactivar la pantalla de las CLI que se envían a los dispositivos y la pantalla de la marca horaria en la ventana de la consola.

Cuando salga de CCA, sus preferencias se guardan en su PC en un archivo llamado `.user_preferences`. Se guarda en esta ubicación:

`C:\Documents and Settings\<`*`username`*`>\.configuration assistant`

Puede copiarlo en otras PC.

La configuración en cada una de estas fichas de la ventana Preferencias se explican en las siguientes secciones, con sus valores por defecto. Si se cambian los valores por defecto, haga clic en **Configurar valores por defecto** para restauralos.

General

En la ficha General, se puede configurar estas preferencias de encuesta e inicio.

Configuración	Descripción
Activar encuesta de red	Por defecto, está desactivada la encuesta de red. Cuando se activa esta opción, CCA periódicamente encuesta a la red para determinar el estado de los dispositivos y descubrir dispositivos nuevos. La información de encuesta se utiliza para actualizar la vista Topología, la vista Panel frontal y muchas de las ventanas de funciones. Cuando la encuesta de red está desactivada, haga clic en el icono **Actualizar** de la barra de herramientas de CCA para activar manualmente la encuesta de red.
Intervalo de encuesta de red	Cuando se activa la encuesta de red, esta configuración especifica con qué frecuencia CCA encuesta la red. Por defecto, son 5 minutos. Esta configuración está inactica cuando se desactiva la encuesta de red.
Intervalo de encuesta de LED	Frecuencia con que CCA encuesta los LED de los dispositivos administrados. En cada intervalo, CCA muestra información de interfaz y RPS con colores de LED en la vista Panel frontal. Puede hacer clic en el botón de la izquierda de la vista para especificar el tipo de información de estado que cada color representa—enlace, velocidad del puerto, el estado a dos caras, o estado de energía. Por defecto, son 3 minutos.

Configuración	Descripción
Intervalo de encuesta de gráfico	Frecuencia con que CCA consulta a los dispositivos administrados para obtener datos de utilización de dispositivos y enlaces. Esta información se utiliza para actualizar el enlace y los gráficos de ancho de banda. Por defecto, son 5 segundos.
Mostrar Vista de topología cuando se conecte a la red	La vista Topología aparece cuando se conecta CCA a un dispositivo. Por defecto aparece marcado.
Mostrar Vista de panel frontal cuando se conecte a la red	La vista Panel frontal aparece cuando se conecta CCA a un dispositivo. Por defecto no aparece marcado.
Mostrar Tablero cuando se conecte a la red	La vista Tablero aparece cuando se conecta CCA a un dispositivo. Por defecto aparece marcado.

Actualizaciones de aplicación

Especifique con qué frecuencia se verifica Cisco.com en búsqueda de una nueva versión de CCA.

En la lista **Verificar actualizaciones de aplicación**, seleccione **Mensual**, **Semanal** o **Nunca**. Si selecciona **Nunca**, CCA no realiza revisiones periódicas. Sin embargo, puede revisar a demanda al seleccionar**Sistema** > **Actualizaciones de aplicación** en la barra de menú.

Servidores proxy

En esta ficha, se muestra si se desea usar servidores proxy para comunicarse con Cisco.com para buscar una versión más reciente de CCA.

Para actualizar CCA a una versión más recientes, siga estos pasos.

PASO 1 Marque **Activar servidores de proxy** para activar comunicaciones a través de servidores de proxy. Cuando usted marca esta casilla, puede utilizar los otros campos de la ficha.

PASO 2 Marque **utilizar servidores proxy para administrar dispositivos** para comunicarse con su red a través de servidores proxy.

PASO 3 Para indicar que el tráfico HTTP utilizará un servidor proxy, introduzca estos valores en los campos **HTTP**:

- La dirección IP o nombre de host del servidor proxy

  Puede utilizar un nombre de host para identificar un servidor de proxy sólo si se ha configurado un servidor DNS para resolver el nombre de host.

- El número del puerto HTTP

PASO 4 Para indicar que el tráfico HTTPS usará un servidor proxy, introduzca los valores adecuados en los campos **HTTPS**.

Archivo de configuración

En esta ficha, se configuran preferencias para hacer copias de seguridad de una configuración guardada en un dispositivo.

Siga estos pasos:

PASO 1 Marque **Guardar configuración en el dispositivo antes de la copia de seguridad** si desea que CCA guarde la configuración en ejecución antes que haga una copia de seguridad de ella como la configuración guardada.

PASO 2 En el campo **Directorio de copia de seguridad**, reemplace la ruta que se utiliza para las copias de seguridad de las configuraciones si desea que éstas se realicen en otra ruta.

Estado

Marque las casillas para las categorías de estado que desea que CCA monitoree.

El **Intervalo de encuesta de estado** determina la frecuencia con que se desea actualizar las mediciones en la ventana Estado y en la ventana Detalles de estado.

Actividad de utilización

La función de seguimiento de la actividad de utilización está diseñada para entregar retroalimentación automáticamente sobre cómo se está utilizando CCA para implementar los dispositivos SBCS de Cisco. Los datos compartidos por esta función ayudan a Cisco a mejorar la calidad del software.

El seguimiento de la actividad de utilización está activada por defecto, según se describe en el Acuerdo de licencia de usuario final (EULA) para CCA. Para ver el EULA, seleccione **Ayuda** > **Acerca de** en el menú principal de CCA y haga clic en el enlace Acuerdo de licencia de usuario final.

Desmarque la opción **Activar recolección de actividad de utilización** para desactivar la recolección y transmisión de datos de utilización de CCA a Cisco.

Cuando se activa esta opción, sólo se recopilan estadístidcas de la siguiente actividad:

- Versión e internacionalización de CCA
- Tipos de dispositivos administrados por CCA
- Versión del software para cada dispositivo administrado (por ejemplo, versión de IOS de Cisco, versión de firware del switch y versión del software de Unity Express de Cisco (CUE).
- Acciones de usuario
  - Inicio de la ventana de funciones
  - Eventos de navegación en fichas de las ventanas de funciones y diálogos
- Cuando CCA aplica una configuración a un dispositivo

  No se guardan detalles de la configuración, sólo que el usuario aplicó un cambio a la configuración.
- Dirección IP pública de la PC en la que CCA está instalado y desde donde se envían los datos.

  Esta es la dirección WAN o IP de Internet mantenida y asignada por su Proveedor de servicios de Internet (ISP) al router o firewall de su sitio.
- Marca horaria para cada evento
- Uso de VLAN
  - Si se usa o no la dirección IP por defecto para la VLAN1 en el UC500 (192.168.10.x). CCA no graba la dirección IP de la VLAN1; sólo verifica si se está usando el valor por defecto.
  - Número total de VLAN
- Uso de Smartport: Tipo de perfiles de Smartport aplicado
- Uso de VPN: Tipos de VPN activados (EasyVPN, VPN sobre SSL o VPN de sitio a sitio). No se da seguimiento de las VPN de teléfonos.
- Uso de enlaces SIP
  - Si está activa el enlace SIP o no
  - Si está activado, el proveedor de enlaces SIP seleccionado

- Utilización inalámbrica
  - Si está activada una inalámbrica o no
  - Tipo de seguridad inalámbrica usada
  - Número total de SSID configurados
- Utilización de la memoria flash del UC500: Espacio disponible y espacio total de la memoria flash en Mbytes

NO se recopila la siguiente información:

- Nombres o direcciones de clientes ni ninguna otra información de identificación
- Números de serie del producto u otros identificadores únicos
- Direcciones IP o nombres de host para dispositivos que están detrás del router o firewall de su sitio
- Números de teléfono o cualquier otra información que pudiera utilizarse para identificar a un cliente o VAR
- Nombres de usuarios o contraseñas de Cisco
- Nombres de usuarios o contraseñas configuradas en el dispositivo

Los datos de actividad de utilización se guardan en un archivo de texto en la PC que está ejecutando CCA y se envía a un servidor que Cisco mantiene en base a las sesiones individuales. Después que se envía la información, se elimina de la PC del usuario.

Se genera una alerta de Notificación de eventos cada vez que se envían datos de actividad de utilización.

Registro

En la ficha Registro, se puede definir las preferencias para la información que se visualizará en los archivos de registro de CCA en la ventana Consola de CCA.

Configuración	Descripción
Contenidos del registro	Esta configuración controla la visualización de la información de la CLI en los archivos de registro y de la marca horaria en la ventana Consola de CCA. ▪ La información de la CLI se muestra en archivos de registro de CCA por defecto. Esta opción se activa por defecto al iniciar la aplicación. Para desactivar la información de la CLI en los archivos de registro, desmarque la opción **Marcar Activar visualización de CLI en el registro**. Si el usuario sale de CCA y vuelve a iniciarlo, esta opción se activará por defecto. ▪ Esta opción se activa por defecto al iniciar la aplicación. Para desactivar la visualización de la información de la marca horaria en la ventana Consola de CCA, desmarque **Activar visualización de la marca horaria en la consola** (para abrir la ventana Consola de CCA, presione la tecla F2). Si el usuario sale de CCA y vuelve a iniciarlo, esta opción se activará por defecto.

Avanzadas

Configure esto desde la ficha Avanzadas.

Configuración	Descripción
Activar sonido de inicio	Marque **Activar sonido de inicio** si desea escuchar el archivo Cisco.wav al inicio.
Activar la vista posterior de CLI de las funciones de voz de IOS	Marque **Activar Vista posterior de CLI para las funciones de voz de IOS** si se desea ver una lista de los comandos de IOS de Cisco enviados al router después que se hagan los cambios de configuración en una ventana de configuración. Los comandos se muestran en una ventana emergente después que se han aplicado los cambios.

Configuración	Descripción
Imagen de fondo del escritorio	Para seleccionar una imagen de fondo diferente, haga clic en **Examinar** y avance hasta la ubicación del archivo deseado en la PC local y haga clic en **Aceptar** o **Aplicar**. Los tipos de imágenes admitidas incluyen .PNG y .JPG. Si la imagen supera el tamaño del escritorio, será recortada. Si la imagen es demasiado pequeña que usará un "mosaico"de pantalla estilo.

Notificación de mensajes del sistema

La ventana Notificación de mensajes del sistema aparece cuando se selecciona **Sistema** > **Notificación de mensajes del sistema** en la barra de menú de CCA.

Se puede recibir notificaciones por correo electrónico de mensajes del sistema que se desee recibir. Los mensajes del sistema pueden ser sobre cualquier evento del sitio de clientes, desde emergencias y alertas (con niveles de gravedad de 0 y 1) hasta mensajes información o de depuración (con niveles de gravedad entre 6 y 7).

Para activar esta función, se debe

- Activar que un servidor SMTP envíe notificaciones por correo electrónico acerca de los mensajes del sistema.
- Crear un nombre de la notificación.

Para configurar notificaciones de mensajes del sistema, siga estos pasos.

PASO 1 En el campo **Servidor de correo electrónico (SMTP)**, indique el nombre del servidor SMTP que enviará las notificaciones.

PASO 2 En el campo **Dirección del remitente**, indique una dirección de correo electrónico para que SMTP la muestre como el remitente de las notificaciones. En terminología de SMTP, esta dirección es la dirección de retorno.

PASO 3 Haga clic en **Probar correo electrónico** para probar la conextión entre el servidor SMTP y la dirección de correo electrónico del remitente. Si el remitente recibe el mensaje de prueba, la conexión está verificada.

PASO 4 Haga clic en **Crear** y utilice la ventana Crear notificación. Consulte **Crear o Modificar Notificaciones del sistema, página 63**.

Cuando haya finalizado, aparece el nombre de la nueva notificación en la Lista de notificaciones y su casilla de verificación Activa queda marcada.

PASO 5 Haga clic en **Aceptar** o **Aplicar**.

Para modificar la información de un nombre de notificación, seleccione el nombre, haga clic en **Modificar**, y use la ventana Modificar notificación.

Para eliminar un nombre de notificación, selecciónelo y haga clic en **Eliminar**.

Crear o Modificar Notificaciones del sistema

Aparece esta ventana cuando se hace clic en **Crear** o **Modificar** en la ventana Notificación de mensajes del sistema. Úsela para especificar:

- Un nombre de notificación
- La dirección de correo electrónico de los receptores
- Los tipos de mensajes, por nivel de gravedad, que los receptores recibirán

Para crear o modificar una notificación del sistema, siga estos pasos:

PASO 1 Indique o edite el nombre en el campo **Nombre de la notificación**.

PASO 2 Indique o edite la dirección de correo electrónico en el campo **Dirección de correo electrónico**. Esta es la dirección en la que los receptores recibirán las notificaciones.

PASO 3 Especifique los tipos de mensajes que los receptores recibirán marcando las casillas al lado de los niveles de gravedad de esos mensajes.

Si se marca un nivel de gravedad mayor que 3, es posible que los receptores reciban más notificaciones de las deseadas.

PASO 4 Haga clic en **Aceptar**.

Utilización de la ayuda en línea

La ayuda en línea de CCA se muestra en una ventana separada del navegador de Internet, que entrega:

- Barra de herramientas con botones de navegación Atrás, Adelante e Inicio, botón Imprimir en PDF y cuadro de texto Buscar
- Enlaces de contenidos e índices a la izquierda
  - Por defecto, se muestra la lista Contenidos. Haga clic en el enlace Índice para ir al índice de ayuda.
  - Haga clic en los iconos Libro para expandir o reducir la lista de temas.
  - Mientras está en la vista Índice, se puede especificar una palabra o frase en el cuadro de búsqueda sobre la lista del Índice para buscar las entradas del Índice.
- Tema actual de ayuda a la derecha

Para obtener mejores resultados, active JavaScript en su navegador Internet Explorer. Si se le solicita en la Barra de información, seleccione la opción para permitir el contenido bloqueado para que se pueda ver y utilizar la navegación de ayuda y los controles de la interfaz.

Acceso a la Ayuda en línea

Para acceder a la ayuda en línea:

- Haga clic en **Ayuda** en una ventana o diálogo
- Presione **F1** para acceder a ayuda para la ventana activa
- Seleccione una de estas opciones del menú Ayuda de la barra de menú en la parte superior de la ventana principal:
  - **Contenidos**. Muestra la introducción al tema CCA.
  - **Noevdades**. Muestra los enlaces a información sobre nuevas funciones en la versión actual y recientes.
  - **Ayuda para la ventana Activo**. Muestra la ayuda en línea para la ventana activa. Si se abren múltiples ventanas, la ventana activa es la ventana que tiene foco actualmente.

Búsqueda de ayuda en línea

Para buscar ayuda en línea, especifique una palabra o frase en el cuadro de búsqueda en la esquina superior derecha de la ventana de ayuda en línea, luego, haga clic en **Ir**. Se admiten coincidencias parciales, pero no se admiten los caracteres y patrones de búsqueda comodines, como (*) y (.).

Una vez que se hace clic en **Ir**, la página se actualiza para mostrar los resultados de la búsqueda.

- Haga clic en un enlace de tema para mostrar el tema que contenga coincidencias con la palabra especificada. Las coincidencias se destacan en esa página.
- Haga clic en el icono para abrir el tema en una nueva ventana, permitiéndolo volver con facilidad a la página de resultados de la búsqueda.

Abrir un PDF de la Ayuda en línea

Haga clic en el botón **PDF** en la barra de herramientas de la ventana Ayuda para abrir un PDF que contenga los contenidos completos de la ayuda en línea en formato PDF.

Esto le permite guardar o imprimir una copia de la ayuda para verla fuera de línea.

Imprimir temas de ayuda

Haga clic en el botón **Imprimir** en la barra de herramientas de Ayuda para imprimir el tema actual.

Para imprimir información en las ventanas de CCA, se puede utilizar el sistema de impresión Java. Consulte **Impresión de ventanas, informes y gráficos de CCA, página 66**.

Impresión de ventanas, informes y gráficos de CCA

Para imprimir una ventana, vista o gráfico de CCA, siga estos pasos:

PASO 1 Asegúrese que el objeto que desea imprimir esté activo.

PASO 2 Seleccione **Sistema** > **Imprimir** de la barra del menú para enviar un archivo a una impresora.

Cuando usted imprime una ventana, la impresión está en formato de informe. En este formato, ninguna información de la ventana está truncada, como puede ocurrir si utiliza la tecla **PrtSc** para imprimir la pantalla. El formato de informe también viene marcado con la hora y las páginas están numeradas.

Notas

- No pueden imprimirse las ventanas del Asistente de configuración de telefonía, Asistente de configuración inalámbrica, Administrador de múltiples sitios, Asistente de configuración de monitoreo de vídeo, Asistente de configuración de seguridad, Asistente de configuración de VPN de teléfonos y Tablero.
- Si el objeto que desea imprimir se inactiva por un mensaje emergente de error, no puede imprimirlo hasta que cierre el diálogo de error y lo active nuevamente.
- Para imprimir una ventana pequeña (una ventana secundaria que se abre cuando usted hace clic en un botón en la ventana principal), ésta debe estar abierta y activa.
- Cuando imprime la vista Topología o Panel frontal, la ventana Vista preliminar (**Sistema** >**Imprimir Vista preliminar**) tiene la opción **Ajustar a la página**. Márquela si desea que la vista se imprima en una sola página.

2

Novedades

Para ver información sobre las nuevas funciones y dispositivos admitidos en Cisco Configuration Assistant, consulte estos temas:

- **Versión actual, página 67**
- **Versiones recientes, página 68**

Versión actual

Versión 3,0.(1)

La versión 3.0(1) de CCA es una versión de mantenimiento que resuelve problemas conocidos y encontrados en CCA 3.0.

Función	Descripción
Configuración de la función de voz	
Estado de movilidad de anexos	Es una nueva ventana para ver la información de teléfonos con Movilidad de anexos, información de su perfil y su estado (**Monitoreo** >**Telefonía** > **Estado de movilidad de anexos**). Esta información es sólo de lectura; para configurar estos parámetros, consulte **Movilidad de anexos, página 345**.

Función	Descripción
Cambios y mejoramientos de la interfaz del usuario	
Fondo de escritorio personalizado	Permite que el usuario especifique una imagen para el escritorio de CCA personalizada en el menú **Sistema**, seleccionando **Preferencias...** y haciendo clic en la ficha **Avanzadas**. Para configurar la configuración de preferencias adicionales para CCA, consulte **Configuración de preferencias, página 55**.

Versiones recientes

Versión 3,0

La versión 3.0 de CCA es una versión mayor del software que incluye estas nuevas funciones y cambios en la interfaz del usuario.

Consulte las *Notas de la versión para Configuration Assistant de Cisco versión 3.0* para obtener una lista de problemas conocidos que se resolvieron en esta versión e información acerca de los paquetes de software y localización para el UC500.

Función	Descripción.
Soporte de dispositivos	
Cisco Modelo 69xx Spoporte para teléfonos IP	CCA 3.0 admite la configuración de los teléfonos IP modelos 6901, 6911, 6921, 6941 y 6961 de Cisco. Se admiten actualizaciones de firmware de teléfonos de arrastrar y soltar para estos nuevos teléfonos.
Paquete de software y localización	
Soporte para la versión 8.1.0 del paquete de software para el UC500	CCA 3.0 admite el paquete de software versión 8.1.0. Para obtener más información, consulte la *Notas de la versión para Configuration Assistant de Cisco versión 3.0*. Consulte **Paquetes de software de UC500, página 550**.
Soporte para el paquete de localización para UC500	CCA 3.0 admite la instalación de archivos de localización por medio de paquetes de localización para el UC500. Los paquetes de localización para el UC500 pueden descargarse desde Cisco.com en www.cisco.com/go/uc500swpk. Cada paquete de localización contiene los archivos de idioma para el teléfono, par el correo de voz, para los tonos de red y las cadencias para una localización determinada. Consulte **Paquetes de software para el UC500, página 551**.
Configuración de la función de voz	
Movilidad de anexos	Activación de la Movilidad de anexos (EM) y configuración del sitio global, perfiles de usuarios de EM y de teléfonos de EM. Esta función permite que los usuarios inicien sesión en cualquier teléfono con EM y puedan acceder a apariencias de línea, buzones de correo de voz y discados rápidos. Consulte **Movilidad de anexos, página 345**.
Anexos flotantes	Agrega anexos que no están asociados con un teléfono físico. Consulte **Anexos flotantes, página 342**.
Notificación de correo de voz	Activa globalmente la notificación de mensajes de correo de voz por correo electrónico o teléfono y configura la notificación al usuario. Consulte **Correo de voz y notificaciones, página 377**.

Función	Descripción.
T.37 Facsímil a correo electrónico	Guarda los facsímiles T-37 como correo de voz y los envía como adjuntos al correo electrónico. **T.37 Facsímil a correo, página 457**.
Límite de tiempo de SNR	Configura el límite de tiempo para la Ubicación con número individual (SNR). La ventana de SNR ahora se ubica en **Configurar** > **Telefonía** > **Usuarios y anexos** > **Usuario y teléfonos**. Consulte **Ubicación con número individual (SNR), página 391**.
Límite de tiempo de parqueo de llamadas y llamada repetida	Especifica la configuración de límite de tiempo y llamadas repetidas para las llamadas parqueadas. Consulte **Parqueo de llamadas, página 415**.
Alerta audible de llamada en espera	Se puede configurar un tono de alerta audible y repetitivo para notificar al usuario cuando una llamada se pone en espera en un teléfono IP de Cisco. Consulte **Ficha Alerta de llamada en espera, página 363**.
Configuración de detalles del puerto FXO	Especifica la configuraciónd detallada del puerto FXO para el tipo de compansión, desconexión supervisora, reversión de baterías, audio y temporizadores. También se puede copiar la configuración del puerto. Consulte **Configuración de puertos FXO, página 313**.
Tono de grabación en vivo	Configura la duración del tono y los intervalos de éste para la grabación en vivo. Consulte **Grabación en vivo, página 454**.
Importación de datos de usuario y teléfonos a granel mejorada	Realiza una importación a granel de datos de usuarios y teléfonos desde el Asistente de configuración de telefonía o la ventana Usuarios y teléfonos. Los procedimientos para preparar e importar los datos de los usuarios han cambiado desde las versiones anteriores. Consulte **Importación de datos de teléfonos para múltiples usuarios (Importación de usuarios a granel), página 336**.

Función	Descripción.
Configuración de red	
Mapeo NAT estático	Si la conexión WAN se configura con una dirección IP estática o PPoE negociada, se puede configurar mapeos de NAT estática. Consulte **Ventana NAT (IP estática o PPPoE con IP estática), página 259**.
Pasos modificados para la creación de VLAN	La interfaz para crear y configurar las VLAN se ha modificado. Se configura el direccionamiento IP para las VLAN en la ventana VLAN y configure la VLAN de voz por defecto. Consulte **VLANs, página 168**.
Mantenimiento	
Localización del UC500, instalación de software y actualización simplificada	Se ha agregado un asistente de instalación de software separado para las actualizaciones del CU500 en **Mantenimiento** > **Actualización de software** > **UC500**. El asistente simplifica la instalación de software y entrega soporte mejorado para su localización. Consulte **Actualizaciones de software, página 552**.
Cambio entre idiomas de CV/ teléfono primario y alternativo	Se ha simplificado la configuración de región. Ahora se puede cambiar entre los idiomas primario y secundario instalado en el UC500 sin tener que volver a instalar CUE. Consulte **Configuración regional para telefonía, página 302** y **Cómo localizar el UC500 (localizaciones diferentes a Inglés de EE.UU.), página 573**.
Carga y descarga de archivos a la memoria flash del UC500	Ahroa la ventana Administración de archivos entrega opciones para cargar y descargar archivos en la memoria flash del UC500. Consulte **Administración de archivos, página 574**.
Activar o desactivar la encuesta de redes	La ficha General en la ventana Preferencias ahora entrega una opción par activar o desactivar la encuesta de redes. Por defecto, está desactivada la encuesta de red. Consulte **General, página 56**.

Función	Descripción.
Cambios y mejoramientos de la interfaz del usuario	
Cambios en los menú de configuración de teléfonos	Los menús de **Configurar** > **Telefonía** se han reorganizado y han cambiado de nombre. Consulte **Usuarios y teléfonos, página 329**. Estos cambios incluyen: ▪ La ventana Voz ahora se llama Usuarios y teléfonos y se ubica en **Configurar** > **Telefonía** > **Usuarios y anexos**. Las fichas Sistema y Red y sus configuraciones asociadas fueron eliminadas de la ventana Voz. La configuración del sistema de voz ahora se configura en la ventana Configuración del sistema en **Configurar** > **Teleonía** > **Sistema**. ▪ La ventana Región ahora se ubica en **Configurar** > **Telefonía** > **Sistema**. ▪ La ventana Ubicación con número individual ahora se ubica en **Configurar** > **Telefonía** > **Usuarios y anexos**. ▪ La ventana Discado rápido del sistema ahora se ubica en **Configurar** > **Telefonía** > **Usuarios y anexos**. Los discados rápidos para los teléfonos de usuarios ahora se configuran en la ventana Usuarios y teléfonos. ▪ La ventana Correo de voz ahora se ubica en **Configurar** > **Telefonía** > **Usuarios y anexos**. ▪ Las ventanas Contestadora automática, Calendarios, ACD básico, Atención nocturna y Grabación en vivo ahora se ubican en **Configurar** > **Telefonía** > **Gestión de llamadas**. ▪ La ventana Configuración de puerto analógico ahora se llama Puertos FXS y se ubica en **Configurar** > **Telefonía** > **Puertos y enlaces**. ▪ Las ventanas Administrador de múltiples sitios y Máximo de llamadas ahora se ubican en **Configurar** > **Telefonía** > **Administración de sitios**.

Versión 2.2.(6)

CCA 2.2(6) es una versión de mantenimiento que resuelve problemas encontrados en CCA 2.2(5) y entrega soporte para el paquete de software para el UC500 versión 8.0.5, que incluye el software de correo de voz para Cisco Unity Express (CUE) versión 8.0.3.

Para mayor información, consulte las *Notas de la versión para Configuration Assistant de Cisco* versión 2.2(6), dispponible en Cisco.com.

Versión 2.2.(5)

La versión 2..2(5) de CCA agrega soporte para estos dispositivos y contiene las siguientes mejoras de las funciones y cambios en la interfaz de usuarios.

Consulte las *Notas de la versión para Configuration Assistant de Cisco versión 2.0 y posteriores* para obtener una lista de problemas conocidos que se resolvieron en esta versión.

Función	Descripción.
Soporte del paquete de software 8.0.4 para el UC500	CCA 2.2(5) admite el paquete de software 8.0.4 de UC500. Para obtener mayor información y versiones de componentes del paquete de software, consulte las *Notas de la versión para Configuration Assistant de Cisco versión 2.0 y posteriores*
Soporte de Windows 7 (versiones de 64 bits y 32 bits)	CCA ahora puede usarse en PC que ejecutan el sistema operativo Microsoft Windows. Se admiten versiones de 64 bits y 32 bits. Para ver limitaciones y advertencias que se aplican a CCA y Windows 7, consulte las *Notas de la versión para Configuration Assistant de Cisco versión 2.0 y posteriores* **NOTA** Debe desactivarse el Control de cuentas de usuario (UAC) de Windows 7 para que funciones las actualizaciones y operaciones de archvios de arrastrar y soltar.
Verificación de la compatibilidad de la versión de CCA	Cuando se inicie CCA, aparece el diálogo Conflictos con la versión de CCA si la versión de CCA que se está usando es más antigua que la versión de CCA que se usó previamente para configurar el sistema. Se puede cerrar el diálogo o seleccionar una actualización a una versión más nueva de CCA. Consulte **Verificación de la compatibilidad de la versión de CCA, página 20**.

Función	Descripción.
Nuevos dispositivos admitidos	Teléfonos IP CCA 2.2(5) agrega soporte para estos modelos de teléfonos IP para pequeñas empresas de Cisco: ▪ SPA Modelo 525G2 de Cisco ▪ Todos los modelos de la serie SPA300 de Cisco. Se admiten actualizaciones de carga de arrastrar y soltar para estos nuevos teléfonos.
Intercomunicador discable	Ahora, se puede configurar intercomunicadores discables usando CCA. Esto se configura en la ficha Anexos de usuario de la ventana Voz (**Configurar** > **Telefonía** > **Usuarios y anexos**>**Usuarios y teléfonos**). Para obtener más información, consulte **Intercomunicador discable, página 370**.
Intercomunicadores de susurros	Ahora, se puede configurar intercomunicadores de susurros usando CCA. Esto se configura en la ficha Anexos de usuario de la ventana Voz (**Configurar** > **Telefonía** >**Usuarios y anexos** > **Usuarios y teléfonos**). Para obtener más información, consulte **Intercomunicador de susurros, página 373**. Los Intercomunicadores de susurros sólo están disponibles en los teléfonos que admiten líneas octales.
Conference Barge, privacidad y anexos compartidos de líneas octales	Ahora se puede configurar Conference Barge con Privacidad usando CCA. cBarge y Privacidad necesitan que se configuren anexos de líneas octales. cBarge y Privacidad se configuran en la ventana Conference Barge (**Configurar** > **Telefonía** > **Funciones de voz** > **Conference Barge**). Los anexos de línea octales compartidos se configuran en la ficha Anexos de usuario de la ventana Voz (**Configurar** > **Telefonía** > **Usuarios y anexos**>**Usuarios y teléfonos**). Para obtener más información, consulte **Conference Barge, página 422**.

Función	Descripción.
Activar o desactivar tonos de unión o abandono de conferencia	Ahora, se puede activar o desactivar la reproducción de tonos cuando quien llama se une o abandona una conferencia multi-partita. Para acceder a esta configuración, seleccione **Configurar** > **Telefonía** > **Funciones de voz** > **Conferencia**. Debe activarse la función Conferencia multi-partita.
Grupos de localización combinados	CCA ahora admite grupos de localización combinados. Esta función permite que los grupos de localización sean miembros de otros grupos de localización. Para acceder a la configuración de los grupos de localización, seleccione **Configurar** > **Telefonía** > **Grupos telefónicos** > **Grupos de localización** en la barra de funciones. Para obtener más información, consulte **Grupos de localización, página 407**.
Anexo de sobrecapa en línea CO	Ahora, se puede configurar un anexo Sobrecapa en una línea CO (Oficina central) usando CCA. Para obtener más información, consulte **Anexo de sobrecapa, página 368**.
Diagnóstico de conectividad de CUE	En la ventana Diagnóstico de conectivada de CUE (**Solución de problemas** > **Diagnóstico CUE** > **Diagnóstico de conectividad de CUE**), se puede verificar la conectividad con el módulo de CUE en el UC500, generar registros, y realizar tareas de recuperación para colocar al módulo en un estado conocido. Para obtener más información, consulte **Diagnóstico de conectividad de CUE, página 634**.
Captura de PCM	En la ventana Captura de PCM (**Solución de problemas** > **Telefonía Diagnóstico** > **Captura de PCM**), se puede realizar una captura de PCM para solucionar problemas de audio tales como mala calidad de voz, audio unidireccioal o ausencia de audio. Para obtener más información, consulte **Captura de PCM, página 631**.

Función	Descripción.
Diagnóstico de registro de enlaces SIP	En la ventana Registro de enlace SIP (**Solución de problemas** > **Diagnóstico de telefonía** > **Registro de enlaces SIP**) se muestra información de registro SIP se entregan herramientas de diagnóstico para solucionar problemas de registro de enlaces SIP. Para obtener más información, consulte **Registro de enlaces SIP, página 625**.
Nuevo comando de AA por defecto	Ahora, el comando **aa_sbcs_v03.aef** es el comando por defecto de la Contestadora automática. Esta versión del comando de AA entrega una opción para transferir las llamadas a un número designado si quien llama no selecciona una acción después que se reproduce tres veces el saludo principal. Para obtener más información, consulte **Configuración de Contestadora automática, página 435**.

Función	Descripción.
Mejoras misceláneas de funciones de telefonía	Ahora, se puede activar o desactivar el bloqueo de llamadas restringidas y configurar permisos de llamadas para teléfonos de área/dispositivos de facsímil. Esto se configura en la ficha Anexos analógicos de la ventana Voz (**Configurar** > **Telefonía** > **Usuarios y anexos**>**Usuarios y teléfonos**). Se ha agregado una opción **Usar como teléfono de teletrabajo** a la ficha Anexos de usuarios. Cuando se marca esta opción, se configura Punto de terminación de medios (MTP) en el teléfono seleccionado. Consulte **Anexos de usuarios, página 330**. Se ha agregado una opción **Permitir llamadas con vídeo** a la ficha Anexos de usuarios de la ventana Voz para los teléfonos que admiten vídeo de punto a punto. Cuando se marca esta opción , se activa la función Cisco Unified Voice Advantage (CUVA) en el teléfono seleccionado. Consulte **Anexos de usuarios, página 330**. Ahora se puede **editar la descripción que aparece en la esquina superior derecha de la pantalla de los teléfonos IP**. Por ejemplo, se puede editar esta configuración para que muestra el número completo de discado directo entrante (DID) en los teléfonos. En las versiones anteriores, CCA siempre mostraba el Nombre y Apellido del usuario del teléfono en esta área. Esto se configura en la ficha Anexos de usuarios en la ventana Voz. Consulte **Anexos de usuarios, página 330**. CCA ahora entrega la capacidad de **desactivar la configuración de los códigos de acceso de función STCAPP** en los teléfonos analógicos controlados por SCCP. Recomendamos que se desactiva los códigos de acceso a funciones STCAPP para evitar conflictos con los códigos de acceso a funciones que se configuran usando los comandos fac en el servicio de telefonía. Para acceder a esta configuración, seleccione **Solución de problemas** > **Telefonía Diagnóstico** > **Teléfonos analógicos SCCP**. Si se desactiva los códigos de acceso de funciones STCAPP no se afecta a los códigos de acceso de funciones configurados usando los comandos fac en el servicio de telefonía, que siempre están activados. Consulte **Teléfonos analógicos SCCP, página 633**.

Función	Descripción.
Soporte de la tecla HLog para los grupos de llamado de ACD básica y regular	Cuando se configura un grupo de búsqueda BACD, uno regular o uno de envío de llamadas, la tecla HLog se agrega a los teléfonos miembros del grupo. Los agentes y miembros de grupos de llamado pueden iniciar o cerrar sesión en el grupo de búsqueda usando la tecla **HLog**. La tecla **HLog** aparece en los teléfonos miembros del grupo de búsqueda cuando una llamada entrante suena en el teléfono miembro. Los usuarios también pueden acceder a esta tecla desde la pantalla principal del teléfono presionando la tecla **más**. La tecla **HLog** reemplaza el uso de DnD (No molestar) . DnD es menos flexible, ya que deja al suscritpor, por lo general, no disponible para todas las llamadas, no sólo las llamadas al grupo de búsqueda.

3

Guía de inicio de la configuración

Lea los temas de esta sección para saber cómo utilizar Configuration Assistant de Cisco (CCA) para conectarse a un sitio de cliente o dispositivo autónomo y comenzar con la configuración. Se analizan los siguientes temas:

- **Crear y administrar sitios de clientes**
- **Conexión a un sitio o dispositivo autónomo**
- **Utilización de Asistentes de configuración de CCA**
  - **¿Cuál Asistente debería usar y cuándo?**
  - **Asistente de configuración de telefonía**
  - **Asistente de configuración de seguridad**
  - **Asistente de configuración inalámbrica**
  - **Asistente de configuración de dispositivo**
  - **Utilidad de configuración para SR520-T1**
  - **Asistente de configuración de VPN de teléfonos**
  - **Asistente de configuración de monitoreo de vídeo**
- **Copia de seguridad y restauración de configuración del dispositivo**
- **Uso de CCA con Cisco Small Business Office Manager, página 122**
- **Recursos para planificar e implementar su solución SBCS**
- **Funciones de SBCS de Cisco admitidas dentro de CCA**

Crear y administrar sitios de clientes

Lea esta sección para saber cómo crear y administrar sitios del cliente utilizando CCA:

- **Acerca de los sitios de clientes**
- **Planificación de sitios de clientes**
- **Crear un nuevo sitio de clientes**

Acerca de los sitios de clientes

Se crea un sitio de cliente para gestionar múltiples dispositivos Smart Business Communications System (SBCS) de Cisco en el mismo grupo lógico, sin importar sus ubicaciones físicas ni el software que esté instalado en ellos. Es posible crear, modificar, eliminar y gestionar múltiples sitios de clientes.

El beneficio de crear un sitio de cliente es que se puede gestionar y monitorear múltiples dispositivos, como un UC500 y SR500 en una sola sesión, sin tener que reconectarse a cada dispositivo en forma separada. La utilización de un sitio de cliente permite que CCA implemente funciones en el nivel de soluciones, como sincronizar las VLAN a través de múltiples plataformas e implementaciones multi-sitios.

Un sitio de cliente puede contener hasta 25 dispositivos de red conectados. Cada dispositivo debe tener asignada una dirección IP. Configuration Assistant de Cisco utiliza la capacidad de reconocimiento automático CDP (Cisco Discovery Protocol) de Cisco y el protocolo Bonjour para encontrar los dispositivos de la red y agregarlos a un sitio. Si los dispositivos no tienen CDP activado, aún es posible crear un sitio y agregar los dispositivos en forma manual.

Con CCA, usted puede comunicarse con todos los miembros de un sitio de cliente en forma segura. Si falla un miembro del sitio, se puede continuar administrando a los demás miembros de ella.

Most types of network devices—routers, switches, wireless LAN controllers—can belong to a customer site. Para ver una lista específica de dispositivos elegibles, consulte las *Notas de versión de Configuration Assistant de Cisco*.

Las siguientes tareas básicas de red se admiten por los miembros del sitio de cliente, incluidos routers y puntos de acceso.

- Gestión de acceso de usuarios
- Actualizar el software

- Cómo guardar una configuración en ejecución
- Copia de seguridad y restauración de una configuración
- Cómo administrar la hora del sistema
- Cómo obtener notificaciones de mensajes del sistema
- Cómo cambiar el número de puerto HTTP
- Cómo obtener un informe de inventario

Planificación de sitios de clientes

Esta sección describe las pautas, requisitos y advertencias que se deben comprender antes de crear un sitio de cliente.

Características de los candidatos y de los miembros

Los miembros son dispositivos de la red que pertenecen a un sitio de cliente. *Candidatos* son dispositivos de red que aún no son parte de un sitio de cliente.

Para unirse a un sitio de cliente, un dispositivo candidato debe

- Ser admitido por CCA
- Tener una dirección IP que sea localizable desde la PC que ejecute CCA
- Tener activado a HTTP o a HTTPS en los puertos por defecto

  Debe estar abierto el acceso a estos puertos si el dispositivo está detrás de un firewall.

Límites del dispositivo del sitio de cliente

El número total de estos tipos de dispositivos no puede ser superior a 25:

- Plataformas de las series UC500 (UC520, UC540 y UC560)
- Switches Small Business Pro de la serie ESW500 de Cisco (todos los modelos y SKU)
- Puntos de acceso inalámbricos AP541N de Cisco
- Switches Catalyst Express CE520
- Routers de la serie 800 de Cisco
- Router de la serie 870 de Cisco

- Routers seguros de la serie SR500 de Cisco
- Dispositivos de seguridad de la serie SA500 de Cisco
- Controladores Wireless Express 526 de Cisco
- Puntos de acceso autónomos Wireless Express AP521 de Cisco. Estos son puntos de acceso autónomos con funciones completas que no necesitan un Controlador de movilidad 526 de Cisco.

No hay límite en el número de teléfonos IP o puntos de acceso. Ligeros puntos de acceso gestionados por un controlador de WLAN en un sitio del cliente. No hay límite para el número de sitios de clientes que CCA puede gestionar.

Además del límite general de 25 dispositivos, existen los siguientes límites por tipo de dispositivo:

- Catalyst Express CE520 and Cisco Small Business Pro ESW500 Series switches—no more than 15.
- Cisco 800 Series routers plus Unified Communications 500 Series platforms—no more than five (5).
- Cisco 526 Wireless Express Controllers—no more than two (2).
- Cisco AP541N wireless access points and Cisco AP521 autonomous access points plus built-in HWIC access points—no more than ten (10).

Si se supera el límite general, o el de tipo de dispositivo, no podrá gestionar el sito de cliente. Debe eliminar dispositivos hasta que no se supere el límite.

Descubrimiento automático de dispositivos

Comenzando con la dirección IP para un dispositivo que se inicia y con los nombres de los puertos para los protocolos HTTPS y HTTP, CCA utiliza CDP (Protocolo de descubrimiento de Cisco) para preparar una lista de candidatos al sitio de cliente que estén dentro de los cuatro saltos de CDP del dispositivo que se inicie. Configuration Assistant de Cisco puede descubrir dispositivos candidatos y miembros en múltiples redes y VLAN, si es que tienen direcciones IP. Consulte la **“Características de los candidatos y de los miembros” section on page 81** para obtener una lista de requerimientos que deben cumplir los dispositivos de red para ser descubiertos.

IMPORTANTE No desactive a CDP en los dispositivos candidatos, miembros ni en ningún otro dispositivo que desee que CCA descubra.

Es posible editar la lista de los dispositivos descubiertos para satisfacer sus necesidades y agregarlos al sitio de cliente. Si CCA no descubre a un dispositivo de la red, es posible agregarlo en forma manual.

Para obtener instrucciones sobre agregar los dispositivos descubiertos a un sitio de cliente o agregarlos manualmente, consulte la **“Adgregar un dispositivo a un sitio de clientes existente” section on page 89**.

Nombres de sitios de cliente

Cuando se crea un sitio de cliente, CCA necesita que se le asigne un nombre. El nombre puede tener hasta 64 caracteres alfanuméricos y no es sensible a las mayúsculas.

Nombres de host

Se puede editar el nombre de host por defecto para unmiembro de sitio de cliente. Esto es útil si se está configurando una implementación multi-sitios o si hay múltiples dispositivos del mismo tipo, por ejemplo, puntos de acceso o switches AP541N. Para editar el nombre de host de un dispositivo gestionado, vaya a **Configurar** > **Dispositivo Propiedades** > **Nombre de host**.

ContraseÃ±as

Cuando se conecte a un sitio de cliente, CCA solicita cada contraseña única que ya se ha asignado a los miembros del sitio de cliente. Configuration Assistant de Cisco intenta utilizar contraseñas para conectarse a otros dispositivos. Se le solicita una contraseña sólo si la contraseña que se indicó previamente no funciona con un dispositivo en particular.

IMPORTANTE Para los dispositivos IOS de Cisco, la contraseña de activación para el dispositivo debe ser la misma que la contraseña usada para iniciar sesión en el diispositivo usando CCA.

Por ejemplo, si un sitio de cliente tiene diez miembros, y cinco de ellos comparten una contraseña, y los otros cinco tienen una diferente, CCA le solicitará contraseñas dos veces, una vez para cada contraseña. Configuration Assistant de Cisco no guarda las contraseñas en su PC y, por ello, solicita las contraseñas cada vez que se intenta conectarse a un sitio de cliente.

Protocolos de comunicación

Configuration Assistant de Cisco utiliza HTTPS, HTTP, Telnet y SSH para comunicarse con los dispositivos. Intenta utilizar HTTPS cuando se descubren dispositivos vecinos y cuando los dispositivos se agregan manualmente a un sitio de cliente. Si falla HTTPS, intenta con HTTP.

El puerto HTTPS está fijo como 443; el valor por defecto del puerto HTTP es 80. Es posible especificar un puerto HTTP diferente cuando se crea un sition de cliente. Posteriormente, se utiliza la ventana Puerto HTTP para cambiar el puerto HTTP. La configuración del puerto tanto para HTTPS como HTTP debe ser igual para todos los miembros de un sitio de cliente.

Información de sitios de clientes

Configuration Assistant de Cisco guarda en su PC toda la información de dispositivos individuales, como la dirección IP, el nombre de host y el protocolo de comunicación. Cuando CCA se conecta a un sitio de cliente, utiliza los datos guardados localmente para volver a descubrir los dispositivos miembros.

Si se intenta utilizar un PC diferente para administrar un sitio de cliente existente, no estará disponible la información acerca de los dispositivos miembros. Es necesario crear el sitio de cliente nuevamente y agregarle los mismos dispositivos.

Crear un nuevo sitio de clientes

La ventana Crear nuevo sitio de clientes aparece cuando se hace clic en **Agregar nuevo sitio** en la ficha Sitios de clientes en la ventana Sitios de clientes o en la ventana Conectar.

Si usted no está familiarizado con CCA o está creando un sitio de clientes por primera vez, consulte **Crear y administrar sitios de clientes, página 80** para averiguar más sobre el propósito y beneficios de crdear sitios de clientes para gestionar dispositivos utilizando CCA.

Utilice esta ventana para crear un nuevo sitio de clientes y descubrir dispositivos que se puedan agregar a un sitio de clientes.

Procedimientos

Para crear un nuevo sitio de cliente, siga estos pasos:

PASO 1 En la sección **Información de sitio de cliente**, especifique un nombre de sitio y una descripción para el sitio de cliente.

El nombre del sitio puede tener hasta 64 caracteres. Puede utilizar los caracteres A-Z, a-z, 0-9, - (guión) y _ (guión bajo).

En el campo opcional **Descripción del sitio** , especifique el nombre de su empresa, su organización o cualquier otro texto identificatorio. El texto aparece como parte del SSID (identificador de conjunto de servicios) recomendada cuando se crea un SSID para su red.

PASO 2 *Opcional.* Haga clic en **Opciones de conexión** si desea

- Introducir un número de puerto HTTP (porque los dispositivos en el sitio de cliente no usarán el valor del puerto por defecto, 80).
- Especificar el modo de acceso para descubrir dispositivos y conectarse al sitio de cliente por primera vez. El valor por defecto es de **Sólo lectura** si ya está conectado a un sitio cuyo modo de acceso de **Sólo lectura**; de lo contrario, es de **Lectura/Escritura**.

Consulte Opciones de conexión, página 87.

PASO 3 En la sección **Agregar dispositivos al sitio**, seleccione **Especificar una dirección IP para el dispositivo** o **Descubrir dispositivos**.

a. Para descubrir y agregar un dispositivo autónomo e individual al sitio, seleccione **Especificar una dirección IP para el dispositivo**, luego especifique la dirección IP del dispositivo que desee que CCA descubra.

b. Para descubrir u agregar múltiples dispositivos, seleccione **Descubrir dispositivos**. Esta tabla muestra las opciones indicadas en el menú **Descubrir dispositivos** , explica la configuración adicional y describe lo que CCA descubre y muestra en la tabla Dispositivos.

Opción	Qué especificar	Lo que CCA muestra
Descubrir dispositivos > utilizando una dirección IP de inicio	La dirección IP de un dispositivo vecino al que desea agregar a su sitio	Información acerca del dispositivos que usted identificó y de los vecinos que descubrió el Protocolo de descubrimiento de Cisco usando un conteo de saltos de 4
Descubrir dispositivos > en una subred	Una dirección IP y una máscara de subred que identifican una subred cuyos dispositivos usted desea agregar al sitio	Información acerca de los dispositivos que descubre en la subred
Descubrir dispositivos > dentro de un intervalo de direcciones IP	Las direcciones IP de inicio y de término cuyo intervalo delimita los dispositivos que usted desea agregar al sitio	Información acerca de los dispositivos que descubre en el intervalo de direcciones IP

PASO 4 Haga clic en **Comenzar**.

PASO 5 Cuando comienza el descubrimiento, el botón **Iniciar** se transforma en el botón **Detener**. Haga clic en él en cualquier momento en que desee interrumpir el proceso de descubrimiento.

Consulte **Descubrimiento automático de dispositivos, página 82** para obtener más información sobre el proceso de descubrimiento de dispositivos.

PASO 6 Especifique las credenciales de inicio de sesión para cada dispositivo cuando se las soliciten. También se le puede solicitar que acepte certificados de seguridad para algunos dispositivos.

IMPORTANTE Para los dispositivos IOS de Cisco, la contraseña de activación para el dispositivo debe ser la misma que la contraseña usada para iniciar sesión en el diispositivo usando CCA.

Para obtener más información, consulte **ContraseÃ±as, página 83**.

NOTA Después de tres intentos fallidos de autentificación, el icono del dispositivo se muestra en color rojo en la vista Topología con el mensaje "Inaccesible: Authorization Failed." Para reintentar la conexión, seleccione **Sistema** > **Conectar**. Se le solitará cerrar la sesión y reiniciar CCA.

PASO 7 Si CCA no descubre un dispositivo que desea agregar al sitio de cliente, repita el Paso 3 con una opción **Descubrir** diferente.

PASO 8 Busque las filas de la tabla Dispositivos para los dispositivos que *no* desea agregar al sitio y anule la selección.

Se puede seleccionar hasta 25 dispositivos en un sitio de cliente. También existen límites sobre el número de ciertos tipos de dispositivos que pueden estar en un sitio de cliente. Consulte **Límites del dispositivo del sitio de cliente, página 81**.

Los teléfonos IP no necesitan agregarse explícitamente a un sitio de clientes.

PASO 9 Haga clic en **Aceptar** para agregar los dispositivos al sitio de cliente.

El nuevo sitio de clientes aparece en la ficha Sitios de clientes.

Opciones de conexión

Esta ventana aparece cuando se hace clic en **Opciones de conexión** en la ventana Crear nuevo sitio de cliente o en la ventana Modificar un sitio de cliente.

- Cuando se crea un sitio de clientes y se descubren dispositivos utilizando una dirección IP inicial, una subred o un intervalo de direcciones IP, CCA utiliza primero el protocolo HTTPS para conectarse. Si falla la conexión por HTTPS, CCA lo intenta nuevamente con HTTP.

- Cuando se utilice la opción Nombre de host/Dirección IP para conectarse a un solo dispositivo, CCA se conecta a éste utilizando el protocolo seleccionado en la ficha Opciones avanzadas. Por defecto es HTTPS.
- En las conexiones posteriores a un sitio de clientes o dispositivo autónomo, CCA utiliza el mismo protocolo que se utilizó durante el descubrimiento del dispositivo.

Se puede modificar el campo **Puerto HTTP** sólo si se está creando un sitio de cliente. El campo debe contener el número del puerto HTTP que CCA usará para comunicarse con los dispositivos en la comunidad.

Si se especificia un número de puerto HTTP que no sea 80, el por defecto, agregue y configure el puerto antes de agregar cualquier dispositivos al sitio. Para cambiar el número del puerto después, utilice la ventana Puerto HTTP.

El número de puerto utilizado para conexiones HTTPS no puede cambiarse, debe ser 443.

Puede seleccionar un modo de acceso y nivel de privilegios sólo si está creando un sitio de cliente. Su selección se utiliza al descubrir dispositivos y al conectarse al sitio por primera vez.

Haga clic en **Aceptar** cuando termine en esta ventana.

Modificar un sitio de cliente

Esta ventana aparece cuando se selecciona un sitio de cliente y se hace clic en **Modificar** en la ficha Sitios de cliente de la ventana Conectar o en la ventana de sitios de cliente.

En la ventana Modificar un sitio de cliente, se puede agregar o quitar dispositivos hacia o desde un sitio de cliente. También se puede

- Hacer clic en **Avanzado** para introducir un nuevo número para el puerto HTTP si cambia este puerto para los dispositivos del sitio de cliente.
- En el campo **Descripción del sitio**, especifique o modifique el nombre de su empresa, su organización o cualquier otro texto identificatorio. El texto aparece como parte del SSID (identificador de conjunto de servicios) recomendada cuando se crea un SSID para su red.

Procedimientos

Para agregar o eliminar dispositivos a un sitio de cliente, siga estos pasos:

PASO 1 En la lista **Descubrir**, seleccione una opción. Luego, complete los campos bajo la lista y haga clic en **Iniciar**. Consulte **Crear un nuevo sitio de clientes, página 85** para obtener información acerca de las opciones para descubrir y agregar dispositivos a un sitio.

PASO 2 Cuando comienza el descubrimiento, el botón **Iniciar** se transforma en el botón **Detener**. Haga clic en él en cualquier momento en que desee interrumpir el proceso de descubrimiento.

PASO 3 Si CCA no descubre un dispositivo que desea agregar al sitio de cliente, repita el Paso 1 con una opción **Descubrir** diferente.

PASO 4 Busque las filas de la tabla Dispositivos para los dispositivos agregados que *no* desea en el sitio de cliente y anule la selección. Hasta 25 dispositivos pueden estar en un sitio de cliente. También existen límites sobre el número de ciertos tipos de dispositivos que pueden estar en un sitio de cliente. Consulte **Límites del dispositivo del sitio de cliente, página 81** para obtener información adicional.

PASO 5 Para eliminar dispositivos que ya están en el sitio de cliente, anule la selección de sus entradas en la tabla Dispositivos.

PASO 6 Haga clic en **Aceptar** para guardar sus cambios y cerrar la ventana.

PASO 7 Seleccione **Inicio** > **Topología Ver** para mostrar la vista Topología. Los iconos de los dispositivos descubiertos recientemente se muestran en la vista Topología.

PASO 8 Para agregar un nuevo dispositivo a un sitio de cliente existente, haga clic con el botón derecho sobre el icono de la vista Topología y seleccione **Agregar al sitio** en el menú emergente.

Adgregar un dispositivo a un sitio de clientes existente

Se puede también agregar un dispositivo a un sitio de cliente existente. Para hacerlo, haga clic con el botón derecho en un icono candidato de vista Topología y seleccione **Agregar al sitio**. Se le solicitará indicar el nombre de usuario y contraseña del administrador para autenticarse.

Visualización y listado de dispositivos en un sitio de clientes

Siga estos pasos para ver y mostrar los dispositivos de un sitio de cliente y verificar que el sitio contenga los dispositivos esperados:

PASO 1 Seleccione **Inicio** > **Topología** para mostrar la vista Topología.

PASO 2 Seleccione **Monitorear** > **Inventario** para mostrar un inventario de los dispositivos del sitio de cliente.

Este resumen incluye números de modelos, números de serie, versiones de software, información de IP y ubicación de los dispositivos.

PASO 3 Seleccione **Inicio**> **Panel frontal** para mostrar la vista del Panel frontal.

PASO 4 Seleccione **Inicio** > **Tablero** para mostrar la vista del tablero del sistema.

Administración de los sitios de clientes

Para administrar sitios de cliente, seleccione **Inicio** > **Sitios de cliente** de la barra de funciones.

En la ventana Sitios de cliente se puede ver una lista de sitios de cliente existentes, crear sitios de cliente, modificar sitios de cliente y eliminar sitios de clientes.

Procedimientos

- Para crear un sitio de cliente, haga clic en **Agregar un nuevo sitio de cliente** para abrir una ventana Crear nuevo sitio de cliente. Consulte **Crear un nuevo sitio de clientes, página 85**.
- Para modificar un sitio de cliente, selecciónelo de la lista y haga clic en **Modificar sitio** para abrir una ventana Modificar sitio de cliente. Consulte **Modificar un sitio de cliente, página 88**.
- Para eliminar un sitio de cliente, selecciónelo de la lista y haga clic en **Eliminar sitio**.

Cuando termine con esta ventana, haga clic en **OK**.

Conexión a un sitio o dispositivo autónomo

Cuando inicia CCA, se abren dos ventanas: la ventana Configuration Assistant de Cisco, que contiene la interfaz del usuario y la ventana Conectar.

También se puede abrir la ventana Conectar seleccionando **Sistema** > **Conectar** en la barra de menú.

Configuration Assistant de Cisco se inicia en modo desconectado: no está conectado a un sitio de cliente o a un dispositivo autónomo. En este modo, usted verá la barra de menú en la ventana CCA, pero sólo una cantidad pequeña de elementos de la barra de funciones. La barra de funciones se crea y completa con las funciones del dispositivo sólo cuando CCA está conectado.

Las siguientes secciones describen cómo usar cada una de las fichas de la ventana Conectar:

- **Ficha Sitios de cliente, página 91**
- **Ficha Nombre de host/Dirección IP, página 93**
- **Ficha Opciones avanzadas, página 94**

Ficha Sitios de cliente

Para gestionar y configurar múltiples dispositivos en su red en una sola sesión, cree un sitio de clientes.

SUGERENCIA Si usted no está familiarizado con CCA o está creando un sitio de clientes por primera vez, consulte **Crear y administrar sitios de clientes, página 80** para averiguar más sobre el propósito y beneficios de crdear sitios de clientes para gestionar dispositivos utilizando CCA.

En la ficha Sitios de cliente, usted puede:

- Crear un nuevo sitio de cliente y conectarse a él
- Conéctese a a un sitio de cliente existente seleccionándolo de una lista.
- Modifique o elimine un sitio de cliente existente.

Para crear y conectarse a un nuevo sitio de cliente, siga estos pasos:

PASO 1 Seleccione la ficha Sitios de cliente en la ventana Conectar y haga clic en Agregar a un nuevo sitio. Aparece el diálogo Crear un nuevo sitio de cliente.

PASO 2 Complete los campos del diálogo Crear un nuevo sitio de cliente, descubra los dispositivos yu agréguelos al sitio como se describe en la sección **Crear un nuevo sitio de clientes, página 85**.

PASO 3 Una vez que se ha creado el sitio de cliente con éxito, aparece en la lista de sitios en la ficha Sitios de clientes de la ventana Conectar.

PASO 4 Haga clic en **Conectar**.

Cuando se conecta a un sitio de clientes, CCA muestra un diálogo Autenticación: Dispositivo que solicita que se especifique cada una de las contraseñas únicas que se han asignado a los miembros de ese sitio.

PASO 5 Especifique las credenciales de inicio de sesión para cada dispositivo cuando se las soliciten. También se le puede solicitar que acepte certificados de seguridad para algunos dispositivos.

IMPORTANTE Para los dispositivos IOS de Cisco, la contraseña de activación para el dispositivo debe ser la misma que la contraseña usada para iniciar sesión en el diispositivo usando CCA.

Para obtener más información, consulte **ContraseÃ±as, página 83**.

NOTA Después de tres intentos fallidos de autentificación, el icono del dispositivo se muestra en color rojo en la vista Topología con el mensaje "Inaccesible: Authorization Failed.” Para reintentar la conexión, seleccione **Sistema** > **Conectar**. Se le pedirá que cierre la sesión y reinicie CCA.

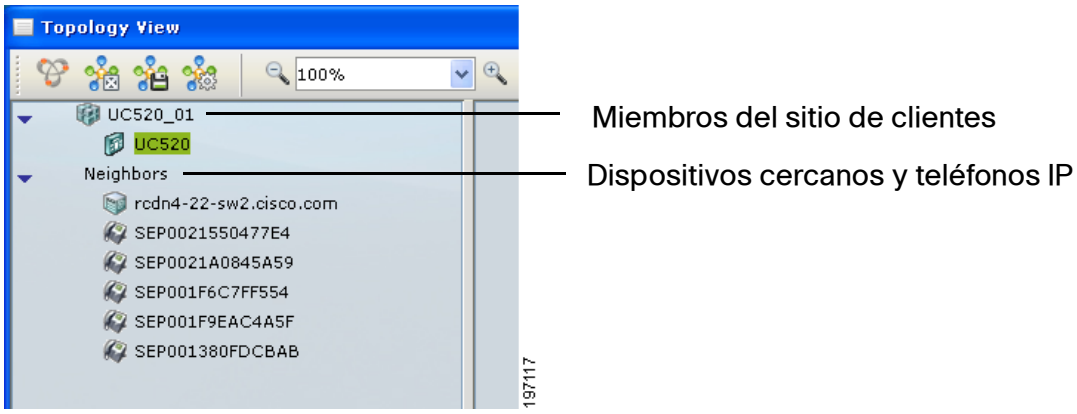
Cuando se haya autentificado con éxito, se establece una sesión de CCA. Sólo puede ejecutarse una sesión a la vez en una PC.

Cuando se está conectado al sitio de clientes, la barra de estado de la parte inferior de la ventana muestra el mensaje “**Descubriendo topología**” mientras CCA descubre los dispositivos y construye la vista Topología. Consulte **Vista Topología, página 34**.

Después que se ha cargado la información sobre topología de red, todo dato de configuración de voz se lee. La barra de estado en la parte inferior d la página muestra el mensaje “**Cargando datos relacionados con voz**.”

Espere hasta que se termine de cargar los datos de configuración de voz antes de poder abrir cualquier ventana relacionada con las funciones Voz o Telefonía.

Los dispositivos que son parte del sitio se indican en el cuadro izquiedo de la vista topología (switches, puntos de acceso y etc.). Los teléfonos IP y los dispositivos que no son parte del sitio de cliente se indican bajo Dispositivos cercanos en el cuadro izquierdo. Aunque los teléfonos IP se indican bajo Dispositivos cercanos, se configuran por medio de CCA.



Para terminar una sesión, cierre la ventana principal de CCA o elija **Sistema** > **Salir**. Se le solicitará guardar cualquier cambio de configuración realizado durante esa sesión a un dispositivo o a todos ellos.

Para modificar la configuración de un sitio existente, seleccione un sitio de cliente de la lista y haga clic en **Modificar**. Consulte **Modificar un sitio de cliente, página 88**.

Para eliminar un sitio de cliente, selecciónelo de la lista y haga clic en **Eliminar**.

Ficha Nombre de host/Dirección IP

Utilice la ficha Nombre de host/Dirección IP cuando desee conectarse y gestionar un dispositivo autónomo especificando su nombre de host o dirección IP.

Para conectarse a un solo dispositivo, siga estos pasos.

PASO 1 Haga clic en la ficha **Nombre de host/Dirección IP** tab, especifique o seleccione un nombre de host o dirección IP para conectarse al dispositivo

PASO 2 Haga clic en **Conectar**.

PASO 3 Especifique el nombre de usuario y contraseña del administrador para su autentificación.

IMPORTANTE Para los dispositivos IOS de Cisco, la contraseña de activación para el dispositivo debe ser la misma que la contraseña usada para iniciar sesión en el diispositivo usando CCA.

Cuando se haya autentificado con éxito, se establece una sesión de CCA. Sólo puede ejecutarse una sesión a la vez en una PC.

NOTA Después de tres intentos fallidos de autentificación, el icono del dispositivo se muestra en color rojo en la vista Topología con el mensaje "Inaccesible: Authorization Failed." Para reintentar la conexión, seleccione **Sistema** > **Conectar**. Se le pedirá que cierre la sesión y reinicie CCA.

Ficha Opciones avanzadas

En la ficha **Opciones avanzadas**, se puede seleccionar si se otorga permiso de **Lectura/escritura** para esta conexión.

Cuando se selecciona Lectura/escritura, se tiene permiso para configurar funciones de redes con CCA. De lo contrario, seleccione Sólo lectura y un nivel de acceso entre 1 y 15.

El modo de acceso por defecto es Lectura/escritura.

Utilización de Asistentes de configuración de CCA

Además de la GUI de configuración en modo experto, CCA entrega varios asistentes de configuración para ayudarle a configurar las soluciones, funciones y dispositivos de SBCS de Cisco.

Para acceder a los asistentes de configuración de CCA, seleccione **Inicio** en la barra de funciones de CCA.

Algunos asistentes sólo están disponibles si los dispositivos necesarios son miembros del sitio de clientes al que está conectado. Por ejemplo, si el sitio de cliente no tiene capacidad inalámbrica, no se muestra la opción del Asistente de configuración inalámbrica.

Consulte las siguientes secciones:

- **¿Cuál Asistente debería usar y cuándo?, página 95**
- **Asistente de configuración de telefonía, página 98**
- **Asistente de configuración de seguridad, página 101**

- Asistente de configuración inalámbrica, página 104
- Asistente de configuración de dispositivo, página 107
- Utilidad de configuración para SR520-T1, página 108
- Asistente de configuración de VPN de teléfonos, página 108
- Asistente de configuración de monitoreo de vídeo, página 111

¿Cuál Asistente debería usar y cuándo?

Cada uno de los asistentes de configuración de CCA está diseñado para automatizar la configuración y mantenimiento de dispositivos, funciones y tipos de implementación específicos. Los asistentes de configuración disponibles se resumen en la siguiente tabla.

Asistente	Lo que este asistente hace...	Cuándo utilizar este asistente	Para saber más
Asistente de configuración de telefonía	Para un sistema SBCS/UC500 de Cisco, el Asistente de configuración de telefonía configura los parámetros básicos de LAN y WAN, la región del sistema, el sistema de telefonía, los enlaces de voz (excepto enlaces SIP), puertos de voz, Contestadora automática, calendarios, usuarios y anexos de teléfonos, enrutamiento de llamadas entrantes y grupos de llamado. El asistente admite todas las plataformas de UC500. Si el UC500 está detrás de un router seguro de la serie SR500, o de un dispositivo de seguridad SA500, el asistente automáticamente ajusta las rutas estáticas y ACL y elimina el firewall del UC500.	Use este asistente sólo para la primera configuración. Este asistente requiere un UC500 con la configuración por defecto de fábrica. Ejecute el Asistente de configuración de telefonía *antes* de ejecutar otros asistentes de configuración de CCA. Si un router seguro SR520-T1 entrega la conexión WAN, se debe ejecutar también la Utilidad de configuración del SR520-T1. Ejecute la Utilidad de configuración del SR520-T1 *antes*antes de ejecutar el Asistente de configuración de telefonía. Consulte **Utilidad de configuración para SR520-T1, página 108**. Para los routers seguros SR520 ADSL/ Ethernet y los de la serie SA500, configure la conexión WAN antes de ejecutar el Asistente de configuración de telefonía.	**Asistente de configuración de telefonía, página 98**

Asistente	Lo que este asistente hace...	Cuándo utilizar este asistente	Para saber más
Asistente de configuración de seguridad	El Asistente de configuración de seguridad se usa para configurar implementaciones sólo de datos en pequeñas empresas con un Dispositivos de seguridad de la serie SA500 como el dispositivo líder de la WAN, junto con switches Small Business Pro y puntos de acceso inalámbricos de Cisco. El asistente configura los parámetros básicos de WAN, LAN y red inalámbrica en el Dispositivo de seguridad de la serie SA500. También automatica la configuración de enlaces para los switches Small Business Pro de la serie ESW 500 oCE520 asociados y sincroniza los perfiles inalámbricos en los puntos de acceso SA500 integrados y AP51N externos que sean miembros del mismo sitio de clientes.	Use este asistente para la primera configuración de una implementación de datos del SA500. También se puede volver a ejecutar el asistente para actualizar esta configuración para una implementación existente. Este asistente también admite un *modo de preparación* que permite configurar previamente los parámetros sion que el SA500 y otros dispositivos estén físicamente conectados a la red. En el modo de preparación, se puede exportar e importar la configuración hacia y desde un archivo local antes de aplicar la configuración final. Ejecute este asistente *antes* de configurar las funciones de seguridad con la Utilidad de configuración del SA500.	**Asistente de configuración de seguridad, página 101**
Asistente de configuración de dispositivo	El Asistente de configuración de dispositivo proporciona instrucciones para conectar y configurar parámetros básicos del dispositivo, como nombre del host y dirección IP para que pueda ser gestionado por parte de CCA. Se admiten los siguientes dispositivos: Switches Catalyst Express CE520 de Cisco Controladores de LAN inalámbrica WLC526 de Cisco para puntos de acceso autónomo AP521 de Cisco Routers seguros SR520 ADSL/Ethernet de Cisco	Use este asistente para la primera configuración de estos dispositivos desde su configuración por defecto de fábrica.	**Asistente de configuración de dispositivo, página 107**
Asistente de configuración inalámbrica	El Asistente de configuración inalámbrica configura y sincroniza la red y perfiles inalámbricos para las implementaciones de voz sobre inalámbrico o sólo datos inalámbricas con múltiples puntos de acceso. El asistente admite puntos de acceso UC500 integrados, AP521 autónomos, teléfonos IP SPA525G y SPA525G2 operando en modo inalámbrico-G y puntos de acceso AP541N.	Use este asistente par la primera configuración y sincronización de perfiles inalámbricos para implementaciones inalámbricas de datos y voz con teléfonos SPA525G y puntos de acceso admitidos. Se puede volver a ejecutar el asistente para actualizar los parámetros de la red y perfiles inalámbricos.	**Asistente de configuración inalámbrica, página 104**

Asistente	Lo que este asistente hace...	Cuándo utilizar este asistente	Para saber más
Asistente de VPN de teléfonos	El Asistente de VPN de teléfonos configura el cliente VPN en los teléfonos IP SAP 525G o SPA525G2 de Cisco que se van a implementar para usarlos en sitios remotos. El Asistente de configuración de VPN de teléfonos no puede usarse en las implementaciones donde la UC500 está detrás de un Dispositivo de seguridad SA500.	Ejecute este asistente en el sitio principal para automatizar la configuración del cliente VPN de teléfonos para los teléfonos IP SPA525G que se implementarán en los sitios remotos. Se puede volver a ejecutar el asistente para actualizar o eliminar la configuración VPN existente de los teléfonos. Se recomienda que se ejecute el Asistente de configuración de VPN de teléfonos *antes* de ejecutar el Asistente de VPN de teléfonos.	**Asistente de configuración de VPN de teléfonos, página 108**
Asistente de configuración de monitoreo de vídeo	El Asistente de configuración de monitoreo de vídeo configura la cámara y asocia las cámaras de vídeo por Internet de la serie PVC2300/WVC2300 de Cisco con los teléfonos IP SPA525G y SPA525G2. Esto permite que los usuarios monitoreen vídeo desde estas cámaras usando el visualizador de cámaras incorporado en los teléfonos IP SPA525G y SPA525G2.	Este asistente puede usarse para la primera configuración de la función de monitoreo de vídeo en los teléfonos SPA525G y cámaras IP de la serie PVC2300/WVC2300 de Cisco. Se puede volver a ejecutar el asistente para actualizar una instalación existente. Ejecute el Asistente de configuración de telefonía *antes* de ejecutar el Asistente de configuración de monitoreo de vídeo.	**Asistente de configuración de monitoreo de vídeo, página 111**
Administrador de múltiples sitios	Use el Administrador de múltiples sitios para configurar y gestionar las implementaciones de datos y voz de múltiples sitios de SBCS de Cisco.	Use el Administrador de múltiples sitios para la primera configuración de una implementación de múltiples sitios de SBCS de Cisco. CCA no reconoce las configuraciones de múltiples sitios fuera de banda existentes. También se puede volver a usar el Administrador de múltiples sitios para agregar, eliminar o editar sitios o para actualizar la configuración de una implementación existente. Se recomienda que se ejecute el Asistente de configuración de telefonía *antes* de ejecutar el Administrador de múltiples sitios.	**Administrador de múltiples sitios, página 489**

Asistente de configuración de telefonía

Para iniciar el Asistente de configuración de telefonía desde la barra de funciones, seleccione **Inicio** > **Asistente de configuración de telefonía**. Si el UC500 del sitio de clientes tiene la configuración por defecto de fábrica, este asistente se inicia en forma automática.

El asistente de configuración de telefonía lo guía por los pasos necesarios para configurar una solución básica de telefonía.

El asistente es para las instalationes iniciales y para casos en los que desee restablecer el UC500 de Cisco a sus valores por defecto de fábrica y reemplazar completamente la configuración actual.

Esta configuración se determina por medio del asistente:

- Configuración de red básica, como tipo de conexión WAN
- Teléfonos, usuarios y anexos primarios
- Grupos de llamado y de envío
- Configuración de enlace (BRI y PRI de ISDN y enlaces analógicos) y números telefónicos
- Plan de numeración específico para la localización
- Ruteo de llamadas entrantes
- Calendario laboral
- Acciones y solicitudes de la Contestadora automática

Cuando se inicie el Asistente de configuración de telefonía, CCA detecta el número de licencias de software instaladas y el paquete de software del UC500 instalado actualmente y/o la versión del software de IOS de Cisco.

El Asistente de configuración de telefonía también admite la importación de datos de usuarios y teléfonos. Para obtener más información acerca de cómo preparar los datos para la importación, consulte **Importación de datos de teléfonos para múltiples usuarios (Importación de usuarios a granel), página 336**.

Los botones para acceder a las ventanas Administración de licencias y Actualizar software en modo experto en el CCA le permiten realizar actualizaciones de licencia y/o software antes de continuar con el asistente. Si se hace clic en estos botones, se cierra el asistente.

Antes de comenzar

Antes de ejecutar el Asistente de configuración de telefonía

- Si la PC que ejecuta CCA tiene más de una interfaz de red (por ejemplo, un NIC doble para la conexión cableada e inalámbrica de la red), asegúrese que sólo uno esté activado.
- Desactive cualquier firewall de terceros o servicios TFTP en la PC que ejecuta CCA.
- Verifique la configuración de seguridad de la red y del firewall en su PC para asegurarse que el tráfico TFTP está autorizado entre la PC y el UC500.
- Asegúrese que la PC que ejecuta CCA esté conectado directamente a un puerto LAN en el UC500 y que haya obtenido una dirección IP del UC500 utilizando DHCP.
- Asegúrese que el sistema UC500 esté con su configuración por defecto de fábrica.
- Para las localizaciones no de EE.UU., descargue e instale archivos de localización en la ubicación adecuada.
- Asegúrese que se ha reunido toda la información indicada en la página de Bienvenida del asistente.
- Si el UC500 estará detrás de un Dispositivo de seguridad de la serie SA500 ó de un Router seguro de la serie SR500, conecte la WAN del UC500 al SA500 ó a la LAN de SR500 antes de ejecutar el Asistente de configuración de telefonía.

Uso del Asistente de configuración de telefonía

Para acceder a este asistente desde la barra de funciones, navegue hasta **Inicio** > **Asistente de configuración de telefonía**.

La configuración que se determine por medio del asistente no se aplica hasta la página final de éste. Para volver a las páginas visitadas previamente de la configuración:

- Utilice el botón **Volver**.
- Use el panel de navegación al lado izquierdo de la página para ir a páginas específicas con una sección de configuración.
- Utilice los enlaces de la página Resumen, y luego haga clic en **Reanudar** para volver a la página de resumen.

Si los cambios que se realizan afectan a otras configuraciones realizadas por medio del asistente, los elementos del menú de navegación destacados en rojo indican errores que deben corregirse antes de continuar.

Una vez que se hace clic en **Aplicar configuración**, se aplicará la configuración seleccionada en el asistente. Si se sale del asistente antes de aplicar la configuración, toda la configuración realizada por medio del asistente se desecha.

Después que se establece la configuración inicial por medio del asistente y se haya verificado que las funciones básicas de voz y trabajo en redes están funcionando en forma adecuada, siga configurando funciones adicionales de voz, seguridad y de trabajo en redes por medio de la GUI de Configuration Assistant de Cisco.

Próximos pasos

Las siguientes funciones de telefonía no se configuran por medio del Asistente de configuración de telefonía:

- Permisos de llamadas para teléfonos individuales (los permisos de llamadas no tienen restricciones para los teléfonos agregados por medio del asistente)
- Bloqueo de llamadas para teléfonos individuales (el bloqueo de llamadas está desactivado para los teléfonos agregados por medio del asistente)
- Intercomunicadores, líneas compartidas, sobrecapas y líneas octales
- Líneas de modo Monitorear y de modo Observar
- Interfaz de enlace SIP
- Distribución básica automática de llamadas (ACD)
- Conferencias con múltiples partes (Ad Hoc/Meet-Me)
- Atención nocturna
- Números personalizados de plan de numeración saliente
- Grupos y prioridades de enlaces
- Discados rápidos del sistema
- Grupos de localización
- Grupos de contestación de llamadas
- Anexos de parqueo de llamadas

- Conferencias
- Movilidad de anexos

Consulte la ayuda en línea u otras secciones de esta guía para obtener información acerca de cómo configurar estas funciones en modo experto utilizando CCA.

Asistente de configuración de seguridad

Para iniciar el Asistente de configuración de seguridad desde la barra de funciones, seleccione **Inicio** > **Asistente de configuración de seguridad**.

NOTA El Asistente de configuración de seguridad está pensado para que se use en implementaciones de sólo lectura con Dispositivos de seguridad de la serie SA500, switches de la serie ESW500 y puntos de acceso AP541. Si se está implementando una solución de telefonía con el UC500, ejecute el Asistente de configuración de seguridad para configurar la red.

El Asistente de configuración de seguridad puede usarse para la primera configuración o editar la configuración existente, como se describe en estas secciones:

- **Visión general**
- **Preparación de la configuración**
- **Descarga e instalación del último firmware para dispositivos SA500, ESW500 y AP541N.**
- **Cómo utilizar el Asistente de configuración de seguridad**
- **Próximos pasos**

Visión general

Los Dispositivos de seguridad de la serie SA500 proporcionan conectividad, enrutamiento, firewall, seguridad, acceso remoto y acceso inalámbrico a la WAN para redes de pequeñas empresas.

El Asistente de configuración de seguridad lo guiará a través de los pasos necesarios para configurar la red inalámbrica para un Dispositivo de seguridad de la serie SA500 de Cisco en una red sólo de datos de una pequeña empresa. El asistente también sincroniza la información del perfil inalámbrico para los pun tos de acceso AP541N e inalámbricos SA500 que sean miembros del sitio de clientes de CCA.

Cuando se aplique la configuración a través del asistente, CCA automáticamente configura el enlace 802.1q y sincroniza la configuración de perfiles invitados y de datos inalámbricas de LAN (WLAN) para los dispositivos Small Business Pro tales como los switches de la serie ESW500 y puntos de acceso AP541N.

Preparación de la configuración

Si CCA detecta que el sitio de cliente al que está conectado no contiene un SA500, el asistente se ejecuta automáticamente en modo de preparación.

En el modo de preparación, se puede configurar previamente los parámetros y guardar su progreso en cualquier punto en el asistente seleccionando **Exportar configuración a archivo**. Para reanudar la configuración, vuelva a ejecutar el asistente y seleccione **Importar configuración desde archivo**.

Una vez que el equipo esté disponible y esté conectado al sitio del cliente, reinicie el asistente, importe la configuración guardada previamente, realice cualquier cambio necesario y aplique la configuración.

Descarga e instalación del último firmware para dispositivos SA500, ESW500 y AP541N.

Si está conectado a un sitio de cliente CCA con un SA500, se muestra la versión actual del firmware del dispositivo SA500. Se requiere una versión V1.1.21 ó posterior del firmware para el SA500.

Para obtener el firmware más reciente desde Cisco.com, siga estos enlaces. Se requiere iniciar sesión en Cisco.com.

- Las descargas de software para los Dispositivos de seguridad de la serie SA500 están disponibles en www.cisco.com/go/sa500software.
- Para los switches de la serie ESW500, un enlace hacia las descargas de software está disponible en www.cisco.com/go/esw500help. Haga clic en la ficha **Recursos** y seleccione el enlace hacia el Firmware en **Firmware y notas de versión**.
- Para los puntos de acceso AP541N, las descargas de software están disponibles en www.cisco.com/go/ap500software.

Cuando haya terminado de descargar el software, haga clic en el botón **Actualizar software** del asistente o seleccione **Mantenimiento** > **Actualizar software** desde la barra de funciones en CCA para abrir la ventana Actualizar software de CCA.

Siga las instrucciones del archivo en línea de CCA para actualizar el firmware para estos dispositivos. Consulte **Actualizaciones de software, página 552**.

Cómo utilizar el Asistente de configuración de seguridad

Para iniciar el asistente desde la barra de funciones, seleccione **Inicio** > **Asistente de configuración de seguridad**.

Siga las instrucciones en pantalla del asistente para configurar estos parámetros:

- Contraseña del administrador (por motivos de seguridad, éste debe cambiarse de la contraseña por defecto de cisco)
- Zona horaria, opción de horario de verano y servidores NTP

  No se puede configurar directamente una hora del sistema en el SA500. Por lo tanto, se necesita un servidor NTP. Los servidores por defecto (0.us.pool.ntp.org y 1.us.pool.ntp.org) se apuntan hacia los Estados Unidos, más que para la zona global.
- Conexión WAN (DHCP, IP estática o PPPoE)
- VLAN de datos
- Rutas estáticas
- Red inalámbrica invitada
- Información de SSID inalámbrico, ID de VLAN y de perfiles para redes de datos e invitadas.

  Cuando se aplica la configuración, el asistente sincroniza esta configuración con el punto de acceso SA520W y con todos los puntos de acceso AP541N de la red. Para sincronizarse, estos puntos de acceso deben ser miembros del sitio de clientes de CCA al que esté conectado.

  La configuración existente se reemplaza con la nueva configuración.

  La seguridad WPA2 con cifrado TKIP + CCMP se configura automáticamente para el tipo de seguridad inalámbrica.

Se puede volver a ejecutar el asistente en cualquier momento para modificar esta configuración.

Próximos pasos

Cuando haya completado el Asistente de configuración de seguridad, se puede hacer clic en el icono del SA500 en la vista Topología y seleccione **Utilidad de configuración** para ejecutar el software de administración del SA500 basado en Internet.

En la Utilidad de configuración del SA500 se puede configurar las funciones de seguridad para el sitio de clientes, como el firewall y la DMZ, filtro de URL, el Sistema de prevención de instrusos (IPS), reenvío de puertos y VPN sobre SSL. Estas funciones no se configuran a través de CCA.

El Gateway ProtectLink de Cisco es un servicio de seguridad en hosts que bloqueda spam y filtra las URL para evitar que contenidos no deseados pasen hacia su red de negocios. Siga las instrucciones de la *Guía de administración de Dispositivos de seguridad de la serie SA500 de Cisco* para obtener un Código de activación y activar los servicios de ProtectLink en el SA500. Para obtener más información, visite www.cisco.com/go/protectlink.

Para obtener nmayor información, consulte la *Guía de administración de Dispositivos de seguridad de la serie SA500 de Cisco*, disponible en la siguiente URL de Cisco.com:

www.cisco.com/go/sa500

Haga clic en la ficha **Recursos** y avance hasta la sección **Documentación técnica** para ubicar la guía de administración y otros enlaces relevantes.

Asistente de configuración inalámbrica

Para iniciar el Asistente de configuración inalámbrica desde la barra de funciones, seleccione **Inicio** > **Asistente de configuración inalámbrica**. La opción Asistente de configuración inalámbrica del menú sólo está disponible si el sitio de clientes al que está conectado tiene capacidad inalámbrica.

- **Visión general**
- **Antes de comenzar**
- **Cómo utilizar el Asistente de configuración inalámbrica**

Visión general

Use el Asistente de configuración inalámbrica para automatizar la configuración de parámetros inalámbricos para múltiples puntos de acceso o para configurar soluciones de voz sobre inalámbrica de SBCS de Cisco con los teléfonos SPA525G o SPA525G2 que operen en un modo inalámbrico G. La configuración de perfiles y redes inalámbricas se sincroniza entre puntos de acceso y teléfonos SPA525G y SPA525G2 que sean miembros del sitio de clientes. Se admiten todos los modelos de UC500.

Se admiten los siguientes dispositivos inalámbricos:

- Puntos de acceso UC500 integrados

- Puntos de acceso Small Business Pro AP541N de Cisco
- Puntos de acceso autónomos AP521 de Cisco

IMPORTANTE Si se activa la agrupación para los puntos de acceso AP541N que sean parte de un sitio de clientes de CCA, no ejecute el Asistente de configuración inalámbrica para configurar estos puntos de acceso.

Si está usando puntos de acceso AP541N de Cisco con teléfonos SPA525G/SPA525G2, siga las pautas de implementación de SBCS descritas en la *Guía de implementación inalámbrica de Voz sobre inalámbrica SBCS 2.0 de Cisco*. Esta guía está disponible en Cisco.com en la siguiente URL:

www.cisco.com/en/US/docs/voice_ip_comm/sbcs/deployment_guides/voice_over_wireless/sbcs_20_vowifi_deployment_guide.pdf

Los teléfonos modelos 7921 y 7925 de Cisco pueden usarse con soluciones de voz sobre inalámbrica SBCS 2.0 que usen puntos de acceso AP541N. Sin embargo, el Asistente de configuración inalámbrica normalmente no sincroniza la configuración de perfiles inalámbricos para estos teléfonos.

Si está usando puntos de acceso autónomos AP 521 de Cisco con teléfonos IP SPA525G/SPA525G2, siga los diseños y pautas de referencia especificados en la *Guía de implementación inalámbrica de SPA525G de Cisco para SBCS de Cisco*. Esta guía está disponible en Cisco.com en la siguiente URL:

www.cisco.com/en/US/docs/voice_ip_comm/sbcs/deployment_guides/spa525g_phone/sbcs_spa525g_wireless_deployment_guide.pdf

Antes de comenzar

El sistema debe cumplir con los siguientes requisitos:

- Se requiere CCA versión 2.2(2) ó posterio para admitir los AP541N por medio del Asistente de configuración inalámbrica.
- Los teléfonos IP SPA525G deben estar ejecutando firmware de versión 7.1.3 ó posterior
- Paquete de software para UC500 7.0 ó posterior
- Los puntos de acceso AP541N deben estar ejecutando firmware de versión 1.8.0 ó posterior.
- Los teléfonos SPA525G/SPA525G2 se que conectarán en forma inalámbrica deben tener una fuente de potencia externa modelo PA100.

Antse de ejecutar el Asistente de configuración inalámbrica, se debe

- Reunir la siguiente información: SSID y contraseñas (claves previamente compartidas) que desee usar para las redes inalámbricas de datos, voz e invitadas.
- Conecte todo punto de acceso externo (AP541N ó AP521) al UC500.
- Conectar todo teléfono SPA525G/SPA525G2 directamente al lado de LAN del UC500 para la sincronización del perfil inalámbrico.
- Crear un sitio de cliente CCA para el UC500, los teléfonos y puntos de acceso.
- Conectarse al sitio de clientes y verificar que los puntos de acceso externo sean miembros del sitio de clientes.

Cómo utilizar el Asistente de configuración inalámbrica

Para ejecutar el Asistente de configuración inalámbrica, conéctese al sitio de clientes que se creó y seleccione **Inicio** > **Asistente de configuración inalámbrica** en la barra de funciones.

Siga las instrucciones en pantalla para configurar estos parámetros:

- Active el modo inalámbrico en los teléfonos SPA525G/SPA525G2.
- Configure SSID, contraseñas (claves previamente compartidas) para las redes inalámbricas de datos y voz.
- Seleccione si se activa o no la transmisión de SSID.
- Active la red invitada, si es necesario, y configure SSID, contraseñas (claves previamente compartidas) y seleccione si se activará la transmisión de SSID.

Las siguientes notas se aplican las ID de VLAN configuradas con el Asistente de configuración inalámbrica:

- La ID de la VLAN de la red de voz de configura como 1 (el valor reservado por CCA).
- La ID de la VLAN de la red de datos de configura como 100 (el valor reservado por CCA).

- La ID de la VLAN de la red invitada de configura como 25 (el valor reservado por CCA).
  - Si ya existe el SSID cisco-guest en un dispositivo del sitio de clientes y su ID de VLAN no está configurada como 25, el SSID cisco-guest existente se elimina y vuelve a crearse, y su ID De VLAN se configura como 25.
  - Si ya existe el SSID cisco-guest en un dispositivo del sitio de clientes y su ID de VLAN ya está configurada como 25, no se modifica su configuración.

El asistente configura automáticamente los parámetros QoS en los puntos de acceso AP541N y el cifrado WPA2-PSK para la seguridad inalámbrica. No se necesita especificar estas opciones.

Se puede volver a ejecutar el asistente en cualquier momento para modificar esta configuración. Cada vez que se ejecute el asistente, éste sobreescribe los valores existentes con la nueva configuración.

Asistente de configuración de dispositivo

Deben configurarse nuevos dispositivos u otros dispositivos que se hayan restablecido a sus valores por defecto de fábrica. Use el Asistente de configuración de dispositivo para dejar a estos dispositivos listos para que CCA los administre. Para iniciar el asistente desde la barra de funciones, seleccione **Inicio** > **Asistente de configuración de dispositivo**. Siga las instrucciones paso a paso de la pantalla para configurar el dispositivo.

NOTA El router seguro SR520-T1 de Cisco tiene su propia utilidad de configuración, la Utilidad de configuración para SR520-T1. Esta utilidad de configuración se inicia automáticamente si el dispositivo SR520-T1 está conectado a un UC500 y tiene su configuración por defecto de fábrica. Consulte **Utilidad de configuración para SR520-T1, página 108**.

Se puede configurar estos dispositivos utilizando el Asistente de configuración de dispositivos:

- Routers seguros SR520 ADSL/Ethernet de Cisco
- Switches CE520 de Cisco
- Puntos de acceso autónomos AP521 de Cisco
- Controlador de LAN inalámbrica WLC526 de Cisco

El punto de acceso inalámbrico de radio única y doble banda AP541N de Cisco no puede configurarse por medio del Asistente de configuración de dispositivos.

Utilidad de configuración para SR520-T1

Si el sitio uncluye un router seguro SR520-T1 y éste tiene su configuración por defecto de fábrica, seleccione **Inicio** > **Utilidad de configuración para SR520-T1** para:

- Configurar la conexión WAN de T1
- Modificar la dirección IP de LAN0 por defecto durante la configuración inicial (*opcional*)
- Ver información de diagnóstico y ejecutar pruebas de ping para verificar conectividad
- Actualización de software del SR520-T1

Para obtener información importante acerca de los requisitos previos y procedimientos paso a paso, consulte la *Guía de inicio rápido para router seguro SR520-T1 Small Business Pro de Cisco* y la nota de la aplicación para la *Configuración de router seguro UC500 y SR520-T1*, disponibles en Cisco.com.

Una vez que se haya configurado la conexión T1, utilice CCA en modo experto para realizar configuraciones adicionles y funciones como NAT, Firewall y DMZ, cuentas de administrador, DNS, nombre de host, NTP, SNMP, rutas estáticas y funciones de seguridad avanzadas (IPS, SSL VPN, y filtro de URL).

Asistente de configuración de VPN de teléfonos

NOTA: El Asistente de configuración de VPN de teléfonos no puede usarse en las implementaciones donde la UC500 está detrás de un Dispositivo de seguridad SA500.

Para iniciar el Asistente de configuración de VPN de teléfonos desde la barra de funciones, seleccione **Inicio** > **Asistente de configuración de VPN de teléfonos**. El elemento Asistente de configuración de VPN de teléfonos del menú sólo está disponible si el sitio de clientes al que está conectado contiene, al menos, un teléfono IP SPA525G o SPA525G2.

- **Visión general**
- **Antes de comenzar**
- **Inicio y utilización del Asistente de configuración de VPN de teléfonos**

- **Activación de VPN de teléfonos en el sitio remoto**
- **Modificación de la configuración de VPN de teléfonos después de la instalación inicial**

Visión general

Use el Asistente de VPN de teléfonos para configurar el cliente VPN en los teléfonos IP SAP 525G o SPA525G2 de Cisco que se van a implementar para usarlos en sitios remotos.

- **En la oficina —** Conecte los teléfonos IP al UC500, configure los anexos de usuarios con CCA y ejecute el asistente para configurar el cliente VPN en el teléfono y configure las cuentas de usuarios VPN en el servidor. Una vez configurado, el teléfono puede desconectarse y enviarse al sitio remoto.
- **En el sitio remoto —** El usuario remoto conecta el teléfono a la red del sitio remoto y activa el cliente VPN en el teléfono. El teléfono inicia una conexión al UC500 sobre un túnel VPN usando los valores previamente configurados. Una vez conectgado a la VPN, el teléfono aparece igual que cualquier otro teléfono en el sitio principal y las llamadas entre el sitio principal y el sitio remoto van sobre la VPN.

Se puede volver a ejecutar el Asistente de configuración de VPN de teléfonos según sea necesario para agregar, editar o eliminar la configuración de cliente VPN en los teléfonos, por ejemplo, para volver a implementar un teléfono en el sitio principal, configurar teléfonos con VPN activada adicionales o cambiar al usuario asociado con el teléfono.

Antes de comenzar

Antes de iniciar el Asistente de configuración de VPN telefónica, su sistema debe cumplir con los siguientes requisitos:

- El servidor VPN sobre SSL y el cliente de Anyconnect deben estar configurados para el sitio. Si no está configurada la VPN sobre SSL, se le pedirá que la configure antes de continuar.

  Se requiere una dirección IP estática para la conexión WAN para la configuración del servidor VPN sobre SSL. Además, se debe activar el modo Túnel total e instale el paquete de clientes Anyconnect de VPN sobre SSL para Microsoft Windows. No se admite el modo de División de arquitectura de túneles para la VPN telefónica.
- Todos los teléfonos IP que van a configurarse para VPN deben tener el último firmware de teléfonos instalado. Se requiere la versión 7.4.2 ó posterior.

- Los teléfonos IP deben estar energizados y conectados al UC500 por medio de un puerto de LAN en el UC500 o por medio de un switch o punto de acceso inalámbrico que esté conectado al UC500.
- Al calcular el número total de conexiones VPN simultáneas requeridas para un sitio de clientes, asegúrese de incluir las conexiones VPN que se usan para las VPN de teléfonos IP.

  Las plataformas UC520 y UC540 admiten un máximo de 10 conexiones VPN simultáneas. La plataforma UC560 admite un máximo de 20 conexiones VPN simultáneas.
- Los teléfonos IP deben estar registrados en el UC500 y mostrar un anexo.
- Los parámetros de telefonía y de red básica deben configurarse para el sitio de clientes, usando el Asistente de configuración de telefonía o la GUI en modo experto de CCA.
- Para mayor facilidad de uso, la configuración de anexos de usuarios, tales como ID de usuarios, contraseñas y botones de teléfonos deben configurarse antes de ejecutar el Asistente de configuración de VPN de teléfonos. Ello se recomienda, pero no es obligatorio. La configuración de anexos de usuarios puede ediatrse aún después de ejecutar el Asistente de configuración VPN de teléfonos.

Inicio y utilización del Asistente de configuración de VPN de teléfonos

Para iniciar el Asistente de configuración de VPN de teléfonos, seleccione **Inicio** > **Asistente de configuración de VPN de teléfonos**.

El asistente descubre los teléfonos IP SPA525G y SPA525G2 conectados al UC500 y muestra la dirección MAC, anexo e ID de usuario de teléfonos para ayudarle a identificar los teléfonos.

Siga las instrucciones en pantalla del asistente para seleccionar los teléfonos y especifique un nombre de usuario y contraseña para la cuenta VPN que se asociará con el teléfono.

A medida que cada teléfono se configfura, la columna Estado se actualiza para indicar su éxito o fallo. Si la configuración no funciona para un teléfono, el asistente continúa con el siguiente teléfono de la lista.

Activación de VPN de teléfonos en el sitio remoto

En el sitio remoto, el usuario de teléfonos debe seguir estos pasos para configurar su teléfono IP y conectarlo a la VPN:

PASO 1 Conecte el teléfono IP a la energía.

PASO 2 Conecte el teléfono a la red del sitio remoto (casa u oficina remota).

PASO 3 Espere que se inice el teléfono y obtenga una dirección IP desde la red en el sitio remoto.

El teléfono se conecta automáticamente al servidor VPN.

Si no desea que el teléfono se conecte automáticamente al servidor VPN, fije la opción **Conectar al iniciarse** en el teléfono IP SPA525G/SPA 525G2 como **DESACTIVADO**. Para acceder a esta configuración, presione el botón **configuración** de la página y vaya a **Información y configuración** > **Configuración de red** > **VPN**.

Para obtener mayor información acerca de los teléfonos IP SPA525G/SPA525G2 de Cisco, vaya a esta URL:

www.cisco.com/go/500phones

Modificación de la configuración de VPN de teléfonos después de la instalación inicial

Se puede volver a ejecutar el Asistente de VPN de teléfonos para configurar la VPN para teléfonos IP admitidos adiconales, editar la configuración de VPN existente o eliminar configuraciones de VPN para los teléfonos.

Antes de eliminar las configuraciones de VPN existentes de los teléfonos, vuelva a ejecutar el Asistente de configuración de VPN de teléfonos y desmarque aquellos teléfonos de la lsita de teléfonos disponibles antes de aplicar la configuración.

Asistente de configuración de monitoreo de vídeo

Para acceder al Asistente de configuración de monitoreo de vídeo desde la barra de funciones, seleccione **Inicio** > **Asistente de configuración de monitoreo de vídeo**.

El elemento Asistente de configuración de monitoreo de vídeo del menú sólo está disponible si el sitio de cliente al que está conectado tiene, al menos, un teléfono IP SPA525G o SPA525G2 y una Cámara de vídeo por Internet de la serie PVC2300 ó WVC2300 de Cisco.

- **Visión general**
- **Antes de comenzar**

- **Preparación de cámaras y teléfonos IP para el monitoreo de vídeo**
- **Inicio y utilización del Asistente de configuración de VPN de teléfonos**
- **Configuración de vídeo de PVC2300/WVC2300**
- **Visualización de vídeo en teléfonos IP SPA525G/SPA525G2**
- **Modificación de la configuración de monitoreo de vídeo después de la instalación inicial**

Visión general

El Asistente de configuración de monitoreo de vídeo lo guiará a través de los pasos necesarios para configurar la cámara y asociar las cámaras de vídeo por Internet de la serie 2300 de Cisco con los teléfonos IP SPA 525G/SPA525G2. Esto permite que los usuarios monitoreen vídeo de las cámaras usando el visualizador de cámaras incorporado en los teléfonos IP SPA 525G/SPA525G2.

Cada teléfono IP SPA 525G/SPA525G2 puede recibir vídeo desde hasta cuatro (4) Cámaras de vídeo por Internet de la serio 2300 de Cisco. Se admiten cámaras modelos PVC2300 (cableadas, PoE) y WVC2300 (inalámbricas, sin PoE).

Se aplican las siguientes limitaciones al monitoreo de vídeo en los teléfonos SPA 525G/SPA525G2:

- Mientras se monitorea vídeo desde el teléfono SPA 525G/SPA525G2, el teléfono puede hacer y recibir llamadas. Sin embargo, las llamadas entrantes no cambian el foco de la pantalla y la única indicación visual será un LED que parpadea asociado con la línea que está recibiendo la llamada. Para responder las llamadas entrantes, simplemente presione el botón de la línea.
- Si está viendo vídeo en el teléfono, la aplicación de vídeo se detiene cuando se hace una llamada saliente y no se reanuda en forma automática.
- No hay integración de audio entre el teléfono IP y las cámaras.
- No se puede activar, simultáneamente, el cliente de VPN y el monitoreo de vídeo en los teléfonos SPA525G/SPA525G2.
- No se admite el Control de puerta de acceso desde el teléfono SPA525G/SPA525G2 usando los puertos GPIO de la parte trasera de la cámara.

Antes de comenzar

Antes de iniciar el Asistente de configuración de monitoreo de vídeo, asegúrese que su sistema cumpla con los siguientes requisitos:

- Los parámetros de telefonía y de red básica se configuran para el sitio de clientes, usando el Asistente de configuración de telefonía o la GUI en modo experto de CCA.
- Los teléfonos IP SPA525G/SPA525G2 debe estar ejecutando firmware versión 7.4.3 ó posterior y deben ser miembros del sitio de clientes de CCA al que se esté conectado. Consulte **Preparación de cámaras y teléfonos IP para el monitoreo de vídeo, página 115**.
- Las cámaras de vídeo por Internet de la serie 2300 de Cisco deben estar ejecutando firmware versión 1.1.4 ó posterior y deben ser miembros del sitio de clientes de CCA al que se esté conectado. Las cámaras debe tener asignada una dirección IP estática.

  Si se estánm usando cámaras WVC2300 (inalámbricas, sin PoE), el SSID por defecto (ciscosb) y la configuración de perfil inalámbrico deben estar definidas para que coincidan con la de los puntos de acceso y del UC500.

  Para obtener mayor información acerca de dónde descargar el firmware de cámaras más reciente y cómo actualizar el firmware de cámaras, consulte **Preparación de cámaras y teléfonos IP para el monitoreo de vídeo, página 115**.
- La PC que ejecute CCA debe estar conectada a un sitio de clientes CCA que contenga al UC500, los teléfonos IP SPA525G/SPA525G2 y las cámaras de la serie PVC2300/WVC2300 de Cisco.

Inicio y utilización del Asistente de configuración de monitoreo de vídeo

PASO 1 Cuando todas las cámaras estén agregadas al sitio de clientes, seleccione **Inicio** > **Asistente de configuración de monitoreo de vídeo** para iniciar el asistente.

PASO 2 Siga las instrucciones en pantalla del asistente para configurar la cámara y los teléfonos IP asociados con las cámaras.

a. Para cada cámara de la lista, se puede editar el nombre de la cámara y su descripción de ubicación, especificar un nombre de usuario y contraseña y especificar un anexo que se va a llamar.

   El nombre de usuario y contraseña configurados por medio del asistente proporcionan acceso administrativo a la cámara por medio de CCA para crear

cuentas con privilegios de Monitoreo en las cámaras que usan los teléfonos IP. El número de teléfonos especificado en el campo **Anexo a llamar** es el número de anexo o de teléfono que se marca cuando un usuario de teléfonos presiona la tecla **Llamar** en su teléfono IP mientras se ve vídeo desde la cámara.

b. Asociación de teléfonos IP SPA525G/SPA525G2 con las cámaras IP. Cada teléfono IP puede asociarse con hasta cuatro (4) cámaras.

PASO 3 Revise la configuración y aplíquela

Las cámaras de vídeo y teléfonos IP asociados se reinician después que se aplica la configuración.

IMPORTANTE Siga las instrucciones de la sección **Configuración de vídeo de PVC2300/WVC2300, página 114** para configurar los parámetros de vídeo para las cámaras que enviarán vídeo a los teléfonos.

Configuración de vídeo de PVC2300/WVC2300

Se debe cambiar la configuración de vídeo MJPEG en las cámaras WVC2300/PVC2300 al formato requerido para la integración con SPA525G.

Para cada cámara, realice estos pasos para configurar los parámetros de vídeo.

PASO 1 En la vista Topología de CCA, haga clic con el botón derecho en el icono de la cámara y seleccione Utilidad de configuración.

PASO 2 En el menú de navegación de la izquierda en la utilidad de configuración de la cámara, seleccione **Audio/Vídeo** > **Vídeo**.

PASO 3 En la sección **Configuración de MJPEG**, configure estos parámetros:

Resolución: 320*240
Máxima velocidad de cuadros: 10 fps
Control de calidad de vídeo: Seleccione **Calidad fija** y configúrela como **Normal**.

PASO 4 Guarde la configuración y salga de la Utilidad de configuración de PVC2300/WVC2300.

IMPORTANTE No puede cambiarse la configuración de MJPEG para la cámara si ésta se encuentra integrada con el teléfono SPA525G/SPA525G2. Si se cambia esta configuración, se evitará que el flujo de vídeo se reproduzca en el teléfono.

Visualización de vídeo en teléfonos IP SPA525G/SPA525G2

Una vez que los teléfonos y cámaras se han reiniciado, siga estos pasos para ver vídeo en los teléfonos IP SPA525G.

PASO 1 En el teléfono IP SPA 525G/SPA525G2, presione el botón **Configuración**.

PASO 2 Use las teclas de flecha hacia arriba y hacia abajo del teléfono para navegar hacia Información y **Configuración** > **Monitoreo de vídeo** y haga clic en el botón de selección central.

PASO 3 Seleccione una cámara de la lista y haga clic en la tecla **Monitoreo**.

PASO 4 Cuando el teléfono se conecta a la cámara y muestra vídeo, presione la tecla **Llamar** para marcar el Anexo de teléfono que se configuró con el asistente.

Modificación de la configuración de monitoreo de vídeo después de la instalación inicial

Para agregar o eliminar teléfonos y cámaras o cambiar la configuración, se puede volver a ejecutar el asistente.

Si se usan cámaras IP inalámbricas, deben configurarse con el mismo SSID que la red de datos en el UC500 y en los puntos de acceso. La configuración SSID inalámbrica puede editarse usando la Utilidad de configuración para PVC2300/WVC2300 o usando CCA en modo experto. Seleccione **Configurar** > **SSID** > **de WLAN inalámbricas** de la barra de funciones para acceder a esta configuración en CCA.

También se puede ver o modificar las propiedades de dispositivos de la cámara, tales como usuarios y contraseñas usando CCA.

Preparación de cámaras y teléfonos IP para el monitoreo de vídeo

Consulte estas secciones para obtener información acerca de la actualización del firmware de cámaras y teléfonos IP y de la preparación de teléfonos y cámaras para el monitoreo de vídeo:

- **Obención del último firmware para teléfonos SPA525G/SPA525G2**
- **Configuración de cámaras de Internet de la serie 2300 de Cisco**

Obención del último firmware para teléfonos SPA525G/SPA525G2

Se requiere la versión 7.4.3 ó posterior del firmware para teléfonos SPA525G para activar el vídeo en los teléfonos SPA525G. Se requiere la versión 7.4.3 ó posterior del firmware para teléfonos SPA525G para los teléfonos SPA525G.

La versión 7.4.3 del firmware para teléfonos SPA525G se entrega en la versión version 8.0.1 del paquete de software del UC500. Para obtener el software para SPA525G, se puede instalar el paquete de software 8.0.1 en el UC500 o descargar la versión 7.4.3 ó posterior del firmware para teléfonos SPA525G desde Cisco.com y use el método de arrastrar y soltar para cargar el firmware al UC500.

Los teléfonos SPA525G2 se despachan de fábrica con la versión 7.4.5 del firmware instalado.

Configuración de cámaras de Internet de la serie 2300 de Cisco

Siga estos pasos para configurar y preparar las cámaras de Internet de la serie 2300 de Cisco para usarlas con el Asistente de configuración de monitoreo de vídeo de CCA. Se necesitará

- Desempacar y preparar el hardware de la cámara.
- Descargar el firmware más reciente para la cámara desde Cisco.com.
- Conectar su PC a cada cámara y ejecutar el CD de instalación que viene con la cámara para realizar la configuración básica.
- Asignar una dirección IP estática y actualizar el firmware de cada cámara.
- Para las cámaras IP WVC (inalámbricas), se debe realizar la configuración de SSID de red inalámbrica para que coincidan con la SSID de datos para los puntos de acceso y el UC500.
- Cree un sitio de clientes en CCA y agregue las cámaras al sitio para que pueda usar CCA para configurar el monitoreo de vídeo en los teléfonos IP SPA525G/G2 de Cisco.

PASO 1 Descargue la versión 1.1.4 ó posterior de las cámaras de vídeo por Internet de la serie 2300 de Cisco hacia la PC que ejecuta CCA.

Se requiere una versión V1.1.4 ó posterior del firmware de la cámara.

Este software está disponible en Cisco.com en las siguientes ubicaciones:

- Páginas de producots PVC2300 y WVC2300 de Cisco (sitio de Cisco sólo para EE.UU.).

- **PVC2300**: www.cisco.com/go/pvc2300software
- **WVC2300**: www.cisco.com/go/wvc2300software

En la ficha Recursos, avance hasta la sección Firmware y haga clic en **Descargar Firmware y aceptar acuerdo de licencia para la Cámara de vídeo por Internet PVC2300 de Cisco - Audio/Poe** o
o

Descargar Firmware y aceptar acuerdo de licencia para la Cámara de vídeo por Internet WVC2300 inalámbrica-G - Audio.

Los archivos se llaman PVC2300_Firmware.zip y WVC2300_Firmware.zip.

- Centro de descarga de software de cisco (requiere iniciar sesión en Cisco.com) en

  http://www.cisco.com/public/sw-center/index.shtml

  En la casilla Seleccionar categoría de producto, seleccione **Seguridad** > **Seguridad física de Cisco** > **Cámaras de vigilancia de vídeo para pequeñas empresa de Cisco (Serie Linksys Business)** y seleccione el modelo de la cámara.

PASO 2 Descomprima los archivos de firmware de la cámara que se descargaron: **PVC2300_Firmware.zip**, **WVC2300_Firmware.zip**.

Cuano de actualice el firmware de la cámara usando CCA, se necesitará el archivo **WVC2300 FW_V111R04.bin** o el archivo **PVC2300 FW_V111R04.bin**, dependiendo del modelo de cámara que esté usando.

PASO 3 Desempaque y prepare el hardware de la cámara como se describe en la *Guía de inicio rápido de la cámara de vídeo con audio por Internet de las series PVC2300, WVC2300 de Cisco*. Esta guía está disponible en Cisco.com en la siguiente URL:

http://www.cisco.com/en/US/products/ps9944/prod_installation_guides_list.html

PASO 4 Conecte las cámaras al UC500 como se describe en la *Guía de inicio rápido* y conecte la energía.

La cámara PVC2300 de Cisco puede conectarse a un puerto PoE en el switch de la serie UC500 ó ESW500. La cámara WVC2300 de Cisco usa un adaptador de energía que se entrega con la cámara.

PASO 5 Siga las instrucciones de la *Guía de inicio rápido de la cámara de vídeo con audio por Internet de las series PVC2300, WVC2300 de Cisco* para usar el CD

de instalación para instalar el software y configure los parámetros básicos de la red.

- Acepte el acuerdo de licencia
- Inicie sesión como administrador (admin/admin es el inicio de sesión por defecto).
- Realice la configuración básica de la cámara (nombre de la cámara, descripción, zona horaria, fecha y hora).
- En la página Configuración de red del programa de Instalación, seleccione **Dirección IP fija** para el tipo de configuración y especifique una dirección IP estática para la cámara (192.168.10.x).

  Por defecto, las cámaras PVC2300 y WVC2300 usan DHCP para obtener una dirección IP. Sin embargo, debe configurarse una dirección IP estática en las cámaras para asegurarse que la dirección IP de la cámara siempre coincida con la dirección IP de la cámara configurada en los teléfonos. El Asistente de configuración de monitoreo de vídeo lee la dirección IP configurada en las cámaras.
- Confirme su configuración y salga del asistente de configuración.
- Si se están configurando cámaras WVC2300 (inalámbricas, sin PoE), siga las instrucciones de la guía de administración de cámaras para realizar la configuración inalámbrica. El nombre de la red inalámbrica (SSID) y la seguridad configurada en las cámaras deben coincidir con el SSID configurado para la red de datos en los puntos de acceso y en el UC500.

PASO 6 Actualice el firmware para cada cámara. Se requiere la versión 1.1.1 ó posterior del firmware.

a. Desde una PC conectada a la red local (LAN), inicie un explorador de Internet y conéctese a la cámara usando la dirección IP estática que se le asignó a la cámara (por ejemplo, 192.168.10.21).

b. Inicie sesión como administrador.

c. Hace clic en **Configuración**de la barra de herramientas.

d. Haga clic en **Administración** > **Firmware**. Se muestra la versión actual. Si la versión es anterior a 1.1.4, haga clic en **Actualizar** y siga las instrucciones en pantalla.

e. Cuando se le solicite seleccionar un archivo de actualización, avance hasta el archivo **WVC2300 FW_V111R04.bin** o hasta el archivo **PVC2300**

FW_V111R04.bin en su PC local, dependiendo del modelo de cámara que esté usando.

f. Repita estos pasos para cada cámara.

PASO 7 Si ya no lo ha hecho, inicie CCA y cree un sitio de clientes de CCA.

PASO 8 Con la PC que ejecuta CCA conectada a la LAN de UC500, conéctese al sitio de clientes que contenga al UC500.

PASO 9 Seleccione **Inicio** > **Topología** para mostrar la vista Topología.

Si las cámaras que se están conectando ya se han actualizado al software correcto, se muestran en la vista Topología.

PASO 10 Haga clic en el icono Actualizar de la vista Topología, luego haga clic con el botón derecho en cada cámara y seleccione **Agregar al sitio**.

Ahora, está listo para iniciar el Asistente de configuración de monitoreo de vídeo. Consulte **Inicio y utilización del Asistente de configuración de monitoreo de vídeo, página 113**.

Copia de seguridad y restauración de configuración del dispositivo

Para acceder a las opciones copia de seguridad y restaurar, seleccione **Mantenimiento** > **Archivo de configuración** en la barra de funciones.

Visión general

Esta sección entrega instrucciones para hacer la copia de seguridad de la configuración de inicio de todos los dispositivos o un solo dispositivo administrado a su PC o una unidad de red y cómo restaurar una configuración previamente guardada.

Además de la configuración de inicio, estos archivos y directorios de la unidad flash de UC500 también se guardan en copia de seguridad y se restauran.

- Configuración de discado rápido del sistema
- archivo vlan.dat (configuración de VLAN)

- Directorios en la memoria flash para las solicitudes BACD, imágenes de escritorio telefónico, medios (archivos de Música en espera) y tonos de llamada.
  - flash:bacdprompts/
  - flash:Desktops/
  - flash:ringtones/
  - flash:media/

Si el UC500 que se está copiando por seguridad aún tiene una estructura de directorio plano, sólo la configuración de inicio, configuración VLAN y discados rápidos se copian por seguridad y se restauran.

Procedimientos

Esta sección cubre los siguientes temas:

- **Copia de seguridad de una configuración, página 120**
- **Para restaurar una configuración desde una copia de seguridad, página 121**
- **Preferencias de copia de seguridad, página 122**

Copia de seguridad de una configuración

Siga estos pasos para hacer copia de seguridad de la configuración de inicio de un dispositivo administrado o de todos los dispositivos:

PASO 1 En la ventana Archivo de configuración, haga clic en la ficha **Copia de seguridad**.

PASO 2 En la lista Nombre de host, seleccione **Todos los dispositivos** o al dispositivo con las configuraciones de inicio que desee copiar.

PASO 3 En el área de texto **Nota de copia de seguridad**, especifique toda información que, posteriormente, le ayude a identificar una configuración con copia de seguridad que desee restaurar.

PASO 4 Haga clic en **Copia de seguridad**.

Las copias de seguridad de la configuración se archiva en el directorio indicado en el campo Directorio de copia de seguridad y el evento se registra en la ficha Restaurar.

SUGERENCIA Es posible eliminar configuraciones archivadas que se acumulen en el directorio de copia de seguridad. El directorio por defecto es C:\Documents and Settings\<*nombre de usuario*>\.configuration assistant\backups.

PASO 5 Haga clic en **Aceptar**.

Para restaurar una configuración desde una copia de seguridad

IMPORTANTE Sólo se puede restaurar una configuración al mismo hardware UC500 en el que se realizó la copia de seguridad. No se admite la migración de configuración entre dos sistemas UC500 separados.

Para restaurar una configuración guardada previamente a la configuración de inicio de un dispositivo administrado, siga estos pasos:

PASO 1 En la ventana Archivo de configuración, seleccione el dispositivo de la lista Nombre de host que desee restaurar.

PASO 2 Haga clic en un botón para determinar el intervalo de configuraciones con copia de seguridad que se muestran en la lista Configuraciones de copia de seguridad.

El botón superior muestra sólo las configuraciones con copia de seguridad del dispositivo que se seleccionó. El botón del medio muestra las configuraciones con copia de seguridad del dispositivo que seleccionó y de cualquier otro dispositivo de su sitio de cliente del mismo tipo de dispositivo. El botón inferior muestra todas las configuraciones con copia de seguridad en el directorio de copias de seguridad.

PASO 3 En la lista Configuraciones con copia de seguridad, seleccione una configuración que se vaya a restaurar.

Observe los contenidos del Área de texto Nota de copia de seguridad para confirmar que la configuración seleccionada es realmente la que se desea.

PASO 4 Haga clic en **Restaurar**.

PASO 5 Haga clic en **Reiniciar** para reiniciar el dispositivo después que se haya restaurado una configuración para él.

Preferencias de copia de seguridad

Para hacer una copia de seguridad en un directorio diferente, haga clic en **Preferencias** en la ventana Archivo de configuración o seleccione **Sistema** > **Preferencias** en la barra de funciones.

En la ventana Preferencias, seleccione la ficha Archivo de configuración y especifique una ruta y directorio diferente.

La ficha también tiene una opción para guardar automáticamente la configuración de ejecución antes de hacer la copia de seguridad. Si no se selecciona esta opción, CCA le solicitará guardar la configuración de ejecución si ésta es diferente de la configuración de inicio.

Uso de CCA con Cisco Small Business Office Manager

Cisco Small Business Office Manager es una aplicación de escritorio sin costo diseñada para un administrador de oficinas de empresas pequeña o para la persona a cargo de TIC. Cisco Office Manager entrega al administrador de la oficina o a la persona a cargo de TIC la posibilidad de realizar tareas operacionales de rutina para el Sistema de comunicaciones Smart Business de Cisco en forma independiente.

Un socio de Cisco configura el sistema, usando CCA, luego personaliza la aplicación Cisco Office Manager y le deja funcionando, lo que permite que el administrador del sitio modifique la configuración de voz y de usuarios del sistema, vea imágenes de vídeo con facilidad de cámaras IP y visualice el estado de la red. Los socios de Cisco pueden trabajar con sus clientes para determinar cuáles funciones podrá controlar el administrador del sitio.

Para conocer más información del productos y ver un enlace para descargar el software para Office Manager de Cisco, visite www.cisco.com/go/officemanager.

La documentación de instalación de Office Manager de Cisco está disponible en la siguiente URL:

www.cisco.com/en/US/products/ps11199/prod_installation_guides_list.html

Recursos para planificar e implementar su solución SBCS

Los siguientes recursos los entrega Cisco para planificar e implementar su solución SBCS:

- Comunidad de soporte para pequeñas empresas de Cisco, página 123
- Smart Designs de Cisco, página 124
- Guías de referencia para plataformas UC540 y UC560 de Cisco, página 124

Comunidad de soporte para pequeñas empresas de Cisco

El sitio Comunidad de soporte para pequeñas empresas (SBCS) entrega recursos para ayudar a VAR y Socios con el diseño, implementación y mantenimiento de las plataformas para SBCS de Cisco.

Para acceder a la Comunidad de soporte para pequeñas empresas de Cisco:

- Dentro de CCA, seleccione **Conexión de socios**> **Comunidad de soporte PE** o
- Abra un navegador web y visite esta URL:

  www.cisco.com/go/smallbizsupport

Éstos recursos incluyen:

- Áreas de soporte organizadas alrededor de un producto, tecnología o país

  Para ir al área de soporte de Smart Business Communications System/ UC500 de Cisco, seleccione **Áreas de soporte**> **Voz y conferencias** > **SBCS/UC500.**
- Foros de discusión (se necesita un inicio de sesión en Cisco.com para publicar mensajes, pero no para leerlos)
- Recursos de capacitación, incluyendo una biblioteca de videos a pedido (VOD) y tutoriales de soporte
- Enlaces a los recursos de soporte de Cisco:
  - Herramientas de soporte de ventas
  - Herramientas de diseño e implementación
  - Guías de configuración y notas de aplicaciones
  - Descargas de software para el UC500
  - Información de garantía de SBCS
  - Universidad PYME (Pequeñas y medianas empresas)

Smart Designs de Cisco

Cisco's SBCS Smart Design documents provide best practices for network solution design and implementation. Estas soluciones simplificadas y probadas previamente para trabajo en redes minimizan la complejidad y los riesgos, mientras que maximizan el éxito de los socios. Para acceder, es necesario iniciar sesión como socio.

Viste esta URL para ver los documentos de Smart Design para SBCS:

www.cisco.com/go/partner/smartdesigns

Guías de referencia para plataformas UC540 y UC560 de Cisco

Para averiguar más acerca de las capacidades y funcioens de las plataformas UC540 y UC560, consulte las siguientes guías, disponibles en Cisco.com.

- *Modelo 560 para pequeñas empresas de la serie Unified Communications 500 de Cisco: Guía de referencia de plataforma*

  www.cisco.com/en/US/prod/collateral/voicesw/ps6788/vcallcon/ps7293/reference_guide_c07-566560.html

- *Modelo 540 para pequeñas empresas de la serie Unified Communications 500 de Cisco: Guía de referencia de plataforma*

  www.cisco.com/en/US/prod/collateral/voicesw/ps6788/vcallcon/ps7293/C78-557768-00_540_platform_reference_guide_DS_v2a.html

Estas guías de referencia de las plataformas cubren los números de partres, interfaces y módulos disponibles, licencias, capacidades básicas de centros de llamados, utilización de recursos de voz para conferencias y transcoding, soporte de localización y especificaciones de hardware para los modelos UC540 y UC560.

Funciones de SBCS de Cisco admitidas dentro de CCA

La *Guía de referencia de funciones del Sistema Smart Business Communications System* proporciona pautas a los socios sobre las funciones que pueden configurarse usando las últimas versiones de CCA. La información se categoriza por Voz, Conmutación, Inalámbrica y Seguridad.

Esta guía está disponible en la ficha Recursos de la página del producto de Resources en la página principal de Cisco Smart Business Communications (www.cisco.com/go/sbcs). Desde dentro de CCA, puede seleccionar **Conexión de socios** > **Guía de funciones de SBCS** para acceder a la guía.

4

Propiedades del dispositivo

Esta sección cubre la configuración de estas propiedades del dispositivo:

- **Su nombre de host**
- **Hora del sistema**
- **Zona horaria (Sólo dispositivos de seguridad SA500)**
- **Puerto HTTP**
- **Usuarios y contraseñas**
- **Acceso remoto a dispositivos (Telnet)**
- **SNMP**

Su nombre de host

Para modificar el nombre de host para un dispositivo:

- Seleccione **Configurar** > **Dispositivo Propiedades** > **Nombre de host** en la barra de funciones.
- Haga clic con el botón derecho en la vista Topología y seleccione **Nombre de host** en el menú emergente.

Visión general

Usted puede darle un nombre de host a un miembro sin nombre de un sitio de la comunidad o puede cambiar su nombre de host.

El nombre de host aparece en las solicitudes del sistema y en el menú desplegable Nombre de host de las ventandas de configuración de CCA.

El cambio de nombre no se hace efectivo inmediatamente. Un mensaje en la barra de estado muestra cuando ha ocurrido el cambio.

Procedimientos

Para modificar el nombre de host para un dispositivo, siga estos pasos:

PASO 1 En la lista **Nombre del host**, seleccione el dispositivo cuyo nombre desea cambiar.

PASO 2 Si seleccionó un dispositivo desde la vista Topología antes de abrir la ventana Nombre de host, el Nombre de host está predeterminado para su selección.

PASO 3 En el campo **Nuevo nombre del host**, especifique un nombre único para el dispositivo. El largo máximo de un nombre de host es de 31 caracteres.

PASO 4 Haga clic en **Aceptar**. La vista Topología se vuelve a desplegar mostrando el nuevo nombre para el dispositivo.

PASO 5 Guarde la configuración (**Configurar** > **Guardar configuración**).

Hora del sistema

Para determinar la configuración de la hora del sistema, seleccione **Configurar** > **Propiedades del dipositivo** > **Hora del sistema**.

IMPORTANTE No se puede configurar las opciones de hora del sistema para el SA500 desde esta ventana. Para configurar la zona horaria y los parámetros del servidor NTP para el SA500, seleccione **Configurar** > **Propiedades del dispositivo**>**Zona horaria**. Consulte **Zona horaria (Sólo dispositivos de seguridad SA500), página 134**.

Visión general

En la ventana Hora del sistema, usted puede

- Configurar manualmente la hora y horario de verano de sus dispositivos de red,
- Configure NTP (protocolo de hora de red) para que los dispositivos soliciten actualizaciones de hora a un servidor NTP, o
- Sincronizar la hora de los dispositivos con la hora de la PC, o con la hora del sistema de un dispositivo en particular.

Por lo general, no es necesario ajustar el reloj del sistema si éste está sincronizado por medio de un mecanismo externo, como NTP. Si no hay otra fuente de hora disponible, debe ajustarse la hora en forma manual. La hora especificada es relativa a la zona horaria configurada.

Consulte estas seccones para obtener instrucciones:

- **Mostrar la hora actual**
- **Ajustar la hora del sistema**
- **Sincronizar hora del sistema**
- **Configurar NTP**

Mostrar la hora actual

La ventana Hora del sistema muestra automáticamente la hora actual: horas (en formato de 24 horas), minutos, zona horaria, mes, día y año para todos los dispositivos de una comunidad.

A continuación se encuentran ejemplos de formatos de fecha y hora:

- Mes, fecha y año: **Agosto/2/2005**.
- Hora y minutos: **9:00** (para 9 A.M) ó **13:00** (para 1 P.M).
- Zona horaria: **(GMT -10:00) Hawaii ,** lo que significa que son 10 horas menos que en el Meridiano de Greenwich.

Ajustar la hora del sistema

En la ventana Hora del sistema, usted puede:

- Ajuste o modifique manualmente la hora en uno o más dispositivos.
- Sincronice la hora en todos los dispositivos de un sitio de la comunidad.

Para ajustar o modificar manualmente la hora del sistema de un dispositivo:

PASO 1 Seleccione la fila para el dispositivo.

PASO 2 Seleccione el mes, día, año, la hora y los minutos correctos de las listas desplegables en las celdas de la fila.

Su selección debe hacerse en formato de 24 horas. Por ejemplo, para 9 A.M., seleccione **09**; para 1 P.M., seleccione **13**; para la medianoche, seleccione **24**.

PASO 3 Seleccione la zona horaria correcta en la lista desplegable.

Se admite la gama completa de las diferencias de la UTC (Universal Time Coordinated). La UTC es lo mismo que el Meridiano de Greenwich. La diferencia (entre la UTC y la zona horaria del switch) puede ser un número negativo o positivo.

Por ejemplo, la Hora estándar del pacífico (PST) tiene una diferencia de -8 horas, lo que significa que está 8 horas por detrás de UTC. Cada zona horaria se visualiza con la diferencia UTC y las principales ciudades o estados de cada región.

PASO 4 Seleccione **Cambiar la hora automáticamente según el horario de verano** para configurar el horario de verano.

El horario de verano automático sólo se admite en los EE.UU., Canadá, Australia y Europa, y comienza el día y hora que se define en la región local.

PASO 5 Haga clic en **Aceptar**.

Para ajustar o modificar manualmente la hora del sistema de múltiples dispositivos:

PASO 1 Seleccione las filas para los dispositivos.

PASO 2 Haga clic en **Modificar**.

PASO 3 Complete la ventana Modificar hora del sistema y haga clic en **Aceptar** para guardar sus cambios. Consulte **Modificar hora del sistema, página 131**.

PASO 4 Haga clic en **Aplicar** en la ventana Hora del sistema para poner en vigencia sus cambios.

PASO 5 Haga clic en **Actualizar** para actualizar la ventana.

Sincronizar hora del sistema

Para sincronizar la hora en todos los dispositivos de una comunidad:

PASO 1 Haga clic en **Sync** para sincronizar todos los dispositivos en el sitio. Para sincronizar dispositivos específicos, seleccione las filas de los dispositivos y haga clic en **Sync**.

PASO 2 Complete la ventana Sincronizar hora del sistema y haga clic en **Aceptar** para guardar sus cambios. Consulte **Sincronizar hora del sistema, página 133**.

PASO 3 Haga clic en **Aplicar** en la ventana Hora del sistema para poner en vigencia sus cambios.

PASO 4 Haga clic en **Actualizar** para actualizar la ventana Hora del sistema.

Configurar NTP

Para configurar un servidor NTP:

PASO 1 En la ventana Hora del sistema, haga clic en NTP.

PASO 2 Complete los campos en la ventna Servidor de hora de red. Consulte **Servidor de tiempo de la red, página 132**.

PASO 3 Haga clic en **Aplicar** para poner en vigencia sus cambios.

PASO 4 Haga clic en **Actualizar** para actualizar la ventana Hora del sistema.

Para obtener más información, consulte estos temas:

- **Modificar hora del sistema, página 131**
- **Sincronizar hora del sistema, página 133**
- **Servidor de tiempo de la red, página 132**

Modificar hora del sistema

Esta ventana aparece cuando se selecciona uno o más dispositivos y se hace clic en **Modificar** en la ventana Sistema.

NOTA Si se seleccionan múltiples dispositivos que tengan diferentes configuraciones, los campos para dichas configuraciones aparecen en blanco. Si los dispositivos seleccionados tienen la misma configuración, ésta aparece.

PASO 1 En el área **Fecha y hora**, seleccione el mes, día y año correcto de las listas desplegables.

PASO 2 Seleccione la hora y los minutos correctos en la lista desplegable.

Su selección debe hacerse en formato de 24 horas. Por ejemplo, para las 9:00 a.m., especifique **09**; para 1:00 p.m., especifique **13**.

PASO 3 Seleccione la zona horaria correcta en la lista desplegable.

Se admite la gama completa de las diferencias de la UTC (Universal Time Coordinated). La UTC es lo mismo que el Meridiano de Greenwich. La diferencia (entre la UTC y la zona horaria del switch) puede ser un número negativo o positivo.

Por ejemplo, la Hora estándar del pacífico (PST) tiene una diferencia de -8 horas, lo que significa que está 8 horas por detrás de UTC. Cada zona horaria se visualiza con la diferencia UTC y las principales ciudades o estados de cada región.

PASO 4 Seleccione **Activar** de la lista desplegable para configurar el horario de verano automático. Seleccione **Desactivar** para desactivar el horario de verano automático.

El horario de verano automático sólo se admite en los EE.UU., Canadá, Australia y Europa, y comienza el día y hora que se define en la región local.

PASO 5 Cuando haya realizado los cambios, haga clic en **Aceptar**. Aparece la ventana Hora del sistema.

Servidor de tiempo de la red

Esta ventana aparece cuando hace clic en **NTP** en la ventana Hora del sistema.

Utilice esta ventana para configurar el cliente NTP (Protocolo de hora de red) si desea que éste envíe solicitudes de hora del día a un servidor NTP en forma regular. El servidor NTP sincroniza al reloj del sistema del cliente con el reloj del servidor cuando el dispositivo así lo solicita.

Para mejorar la seguridad, es posible configurar autentificación de NTP. Cuando se configura autentificación NTP, el dispositivo actualiza la hora sólo si un servidor entrega la autentificación correcta. Para que la autentificación funcione bien, primero, se debe obtener la información clave de parte del administrador del servidor y especificarla en los campos de Autentificación NTP.

Para configurar que los dispositivos reciban actualizaciones de hora desde un servidor NTP y para configurar la autentificación NTP, debe hacer lo siguiente:

PASO 1 En el campo **Dirección IP**, especifique la dirección IP del servidor de hora.

PASO 2 *Opcional*: En el campo **ID de clave**, especifique la clave de autentificación que debe usarse para enviar los paquetes al servidor. Especifique un número entre 1 y 4294967295.

PASO 3 *Opcional*: En el campo **Valor clave**, especifique la clave secreta. Especifique hasta 32 caracteres imprimibles, excluyendo espacios, y los símbolos !, ", #, $, }, |, y ~.

PASO 4 *Opcional*: En el campo **Tipo de cifrado**, especifique el número usado para cifrar el valor de la clave. Especifique un número entre 1 y 4294967295.

PASO 5 Haga clic en **Aceptar** para cerrar la ventana Servidor de hora de red y volver a la ventana Hora del sistema.

Sincronizar hora del sistema

Esta ventana aparece cuando se hace clic en **Sincronizar** o cuando se selecciona uno o más dispositivos y se hace clic en **Sincronizar** en la ventana Hora del sistema.

Visión general

Esta ventana muetra la hora actual de la PC.

Es posible sincronizar la hora del sistema en los dispositivos seleccionados con la hora actual de la PC, o se puede sincronizar la hora del sistema de un dispositivo específico. También es posible sobreescribir la configuración de zona horaria de los dispositivos seleccionados.

Por ejemplo, si se sincroniza la hora del sistema de un dispositivo en Nueva York con la configuración de hora de un dispositivo en San José que tiene una hora de 1 p.m. (PST), después de realizar la sincronización, el dispositivo en Nueva York muestra la nueva hora; 4 p.m. EST. Sin embargo, si se selecciona la casilla de verificación **Sobreescribir zona horaria local**, el dispositivo de Nueva York tendrá la nueva hora de 1 p.m. PST (la misma que el dispositivo en San José). Se sobreescribe la hora local.

Procedimientos

Para sincronizar la hora del sistema de los dispositivos seleccionados con la hora actual de la PC:

PASO 1 Seleccione **Sincronizar con PC**.

PASO 2 Seleccione **Sobreescribir zona horaria local** si desea sobreescribir la zona horaria local de los dispositivos seleccionados.

PASO 3 Haga clic en **Aceptar** para guardar los cambios y volver a la ventana Hora del sistema.

Para sincronizar la hora del sistema de los dispositivos seleccionados con la hora del sistema de un dispositivo específico:

PASO 1 Seleccione **Sincronizar con dispositivo**.

PASO 2 Seleccione el dispositivo (con el que desea utilizar la sincronización) en la lista desplegable.

PASO 3 Seleccione **Sobreescribir zona horaria local** si desea sobreescribir la zona horaria local de los dispositivos seleccionados.

Haga clic en **Aceptar** para guardar los cambios y volver a la ventana Hora del sistema.

Zona horaria (Sólo dispositivos de seguridad SA500)

La ventana Administración de la zona horaria aparece cuando se selecciona **Configurar** > **Propiedades de Dispositivo** > **Zona horaria** en la barra de funciones. Esta opción sólo está disponible si se está conectado a un dispositivo de seguridad autónomo de la serie SA500 o se encuentra uno presente en el sitio del cliente CCA.

Visión general

En la ventana Administración de la zona horaria, usted puede:

- Configurar la Zona horaria del SA500
- Seleccionar si se desea ajustar automáticamente el horario de verano
- Especificar si se utilizará los servidores NTP por defecto para las actualizaciones de hora del sistema o especificar hasta 2 servidores NTP personalizados.
- Ver la hora actual del SA500

No se puede configurar manualmente una hora del sistema en el SA500.

Procedimientos

Para administrar la configuración de Zona horaria en el SA500, complete la configuración como se describe en la siguiente tabla, luego haga clic en **Aceptar** o **Aplicar**.

Configuración	Descripción
Su nombre de host	Nombre de host del SA500 que se está configurando. P0r defecto es SA500.
Zona horaria	Seleccione la zona horaria correcta en la lista desplegable. Se admite la gama completa de las diferencias de la UTC (Universal Time Coordinated). La UTC es lo mismo que el Meridiano de Greenwich. La diferencia (entre la UTC y la zona horaria del switch) puede ser un número negativo o positivo. Por ejemplo, la Hora estándar del pacífico (PST) tiene una diferencia de -8 horas, lo que significa que está 8 horas por detrás de UTC. Cada zona horaria se visualiza con la diferencia UTC y las principales ciudades o estados de cada región.
Ajute automático del horario de verano	Cuando se marca esta casilla, la hora del sistema del SA500 se ajusta automáticamente para el horario de verano. El ajuste automático del horario de verano sólo se admite en los EE.UU., Canadá, Australia y Europa, y comienza el día y hora que se define en la región local.
Uso de servidores NTP por defecto	Configure el SA500 para recibir actualizaciones de hora desde los servidores NTP (Protocolo de hora de redes). Los servidores por defecto son `0.us.ntp.pool.org` y `1.us.ntp.pool.org`.
Uso de servidores NTOP personalizados	Cuando se marca esta opción, se puede especificar hasta dos servidores NTP personalizados para utilizarlos para actualizaciones de hora.

Configuración	Descripción
Servidor NTP 1 **Servidor NTP 2**	Si se marca Usar servidores NTP personalizados, especifique el nombre de host o dirección IP pública de los servidores NTP en estos campos.
Hora actual	Visualización de sólo lectura de la hora y fecha actual del SA500; por ejemplo, Sábado, Enero 01, 2010, 22:24:25 (GMT +0000).

Puerto HTTP

Para cambiar el número del puerto HTTP para todos los dispositivos de un sitio de cliente, seleccione **Configurar** > **Propiedades del dispositivo**>**Puerto HTTP** en la barra de funciones.

Visión general

Configuration Assistant se conecta a todos los dispositivos de un sitio de cliente por medio de un puerto HTTP o HTTPS.

- Se puede cambiar el número de puerto HTTP, pero no el de un puerto HTTPS.
- Para HTTPS, siempre se utiliza el valor por defecto de 443.

HTTPS asegura que las comunicaciones entre Configuration Assistant y los dispositivos administrados estén cifradas. Se puede utilizar HTTPS sólo con una imagen criptográfica de IOS de Cisco.

La primera vez que se conecte con HTTPS, usted verá una alerta. Éste le pregunta si aceptará un certificado que afirma que el dispositivo conectado es un sitio fiable. Las opciones son **Sí**, **No**, **Siempre** y **Ver certificado**.

Responda **Sí** o **Siempre** para continuar. Si su respuesta es **Siempre**, no será alertado en las sesiones posteriores de Configuration Assistant.

Cuando se utiliza HTTPS, podrá observar un icono en la barra de estado.

Procedimientos

Para configurar el puerto HTTP, siga estos pasos:

PASO 1 Especifique un número de puerto distinto en el campo **Puerto HTTP**. El número de puerto por defecto es 80. El rango de otros números de puerto válidos va desde 1025 a 65535.

Haga clic en **Aceptar**. El nuevo número de puerto HTTP se propaga a todos los miembros de la comunidad.

Usuarios y contraseñas

Para configurar las contraseñaas y asociar las contraseñaas con los nombres de usuarios y niveles de privilegio, seleccione **Configurar** > **Dispositivo Propiedades** > **Usuarios y contraseñas**.

Visión general

Usted puede administrar el acceso a CCA configurando contraseñas solas o contraseñas pareadas con nombres de usuarios. También puede asociar un nivel de privilegio con una contraseña y nombre de usuario para administrar el acceso según el usuario.

Dependiendo del tipo de dispositivo que se está configurando, pueden asignarse diferentes tipos de privilegios.

- Para los dispositivos de seguridad SA500 de Cisco Small Business Pro, los niveles de privilegios incluyen Invitado (acceso de sólo lectura), Administrador, y Usuario de VPN sobre SSL.
- Para los puntos de acceso AP541N de Cisco:
  - No se puede crear usuarios adicionales ni modificar el nombre de usuario administrativo por defecto (cisco) ni el nivel de privilegios (Administrador).
  - Sólo se puede modificar la contraseña del administrador por defecto (cisco).
- Para las cámaras Business Internet modelos PVC2300 y WVC2300 de Cisco:

  - Se aplican diferentes niveles de privilegios (Administrador, Monitor y Visualizador).
  - No se puede modificar el nombre de usuario por defecto del adminsitrador (admin), pero se pueden crear usuarios adicionales con privilegios de administrador.
- Para el UC500 y otros dispositivos basados en IOS de Cisco, los niveles de privilegios varían de 1 a 15:
  - El nivel de privilegio 15 le otorga acceso de lectura y escritura. Los usuarios en este nivel pueden ver y configurar todas las opciones en CCA.
  - Los niveles de privilegio desde el 1 al 14 le otorgan acceso de sólo lectura. Se muestran las opciones en la barra de funciones, barra de herramientas, menús emergentes y ventanas de funciones que pueden cambiar la configuración de un dispositivo.

Para configurar las contraseñas y asociar las contraseñas con los nombres de usuarios y niveles de privilegio, utilice la ventana Usuarios y contraseñas.

Procedimientos

En la ventana Usuarios y contraseñas, usted puede:

- **Cómo otorgar acceso a todos los dispositivos del sitio**
- **Gestión del acceso a un dispositivo específico**

Comience seleccionando **Todos los dispositivos** o uno específico de la lista **Nombre de host**.

Haga clic en **Aceptar** cuando haya finalizado de configurar al servidor.

Cómo otorgar acceso a todos los dispositivos del sitio

Para otorgar acceso a todos los dispositivos del sitio del cliente, siga estos pasos:

PASO 1 En el campo **Nombre de usuario de admin**, especifique el nombre de usuario que utilizará un administrador para tener acceso a todos los dispositivos de la comunidad.

PASO 2 En el campo **Contraseña**, introduzca la contraseña que usará el administrador. La entrada está cifrada y aparece como estrellas.

PASO 3 Especifique la contraseña de vista en el campo **Confirmar Contraseña**.

Gestión del acceso a un dispositivo específico

NOTA Las opciones de acceso a Nombre de usuario, Contraseña y Dispositivos varían dependiendo del dispositivo seleccionado. Si no se muestra una fucha para un dispositivo, éste no admite dicha opción.

Utilice estas fichas para otorgar acceso a un dispositivo específico:

- **Nombre de usuario/Contraseña local**, para asociar nombres de usuarios y contraseñas con niveles de privilegios
- **Autentificación HTTPS**, para especificar si los usuarios ingresan tanto el nombre de usuario como la contraseña o sólo una contraseña para acceder a Configuration Assistant
- **Activar contraseña**, para asociar contraseñas con niveles de privilegios
- **Contraseña de la consola/Telnet**, para asociar las contraseñas con la línea de la consola y sesiones de Telnet

Nombre de usuario/Contraseña local

Esta ficha muestra los nombres de usuarios, contraseñas y sus niveles de privilegio asociados. Los usuarios con un nombre de usuario y contraseña pareados en esta ficha tienen acceso a CCA en el nivel de privilegio asociado.

Las opciones de configuración de nomre de usuario y contraseña varían, dependiendo del dispositivo que se está configurando.

Para los puntos de acceso AP541N de Cisco:

- No se puede crear usuarios adicionales ni modificar el nombre de usuario administrativo por defecto (cisco) ni el nivel de privilegios (Administrador).
- Sólo se puede modificar la contraseña del administrador por defecto (cisco).

Para especificar un nuevo registro de acceso de usuario; un nuevo nombre de usuario, contraseña y nivel de privilegios, haga clic en **Crear** y utilice la ventana Crear nombre de usuario/contraseña local. Consulte **Crear usuario, página 141**.

Para modificar el nivel de la contraseña o de los provilegios, selecciónelo, haga clic en **Modificar**, y utilice la ventana Modificar nombre de usuario/contraseña local.

Para eliminar un registro de acceso de usuario, selecciónelo, y haga clic en **Eliminar**.

Autentificación HTTPS

En esta ficha, haga clic en **Activar contraseña** si quiere que los usuarios accedan al dispositivo seleccionado especificando sólo una contraseña. Haga clic en **Nombre de usuario/Contraseña local** si quiere que los usuarios introduzcan tanto la contraseña como el nombre de usuario.

Asegúrese también de utilizar la ficha **Activar contraseña** para configurar contraseñas o la ficha **Nombre de usuario/Contraseña local** para configurar los nombres de usuario y contraseñas.

Activar contraseña

Esta ficha muestra los niveles de privilegio y contraseñas. Los usuarios que ingresan una contraseña que está en esta ficha tienen acceso a Configuration Assistant en el nivel de privilegio asociado.

Para crear una nueva contraseña y el nivel de privilegio asociado, haga clic en **Crear**, y utilice la ventana Crear contraseña de activación.

NOTA Si existe la contraseña para cada nivel de privilegio desde el 1 al 15, se desactiva el botón **Crear**.

Para modificar una contraseña, selecciónela, haga clic en **Modificar**, y utilice la ventana Modificar la contraseña de activación. Consulte **Modificar habilitar contraseña, página 142**.

Para eliminar una contraseña, selecciónela, y haga clic en **Eliminar**. Tanto la contraseña como su nivel de privilegio se eliminan de la ficha.

Contraseña de la consola/Telnet

Esta ficha muestra las contraseñas que están asociadas con la línea de la consola y las sesiones de Telnet.

En una sesión de Telnet, una contraseña de Telnet le otorga a los usuarios acceso de sólo lectura al dispositivo. Ellos no pueden configurarlo. Cuando acceden al dispositivo por telnet, se les solicita la contraseña que ellos comparten. No se les solicita indicar su nombre de usuario. Si no se especifica una contraseña de Telnet, o se la elimina, se les pide a los usuarios que indiquen su nombre de usuario y contraseña en la ficha **Nombre de usuario/contraseña local**.

Al especificar la contraseña de la consola los usuarios obtienen acceso de lectura y escritura. Si creó una contraseña de activación, los usuarios deben especificarla en lugar de la contraseña de la consola para obtener acceso de lectura y escritura.

Para crear contraseñas o para modificarlas, ingréselas en el campo **Contraseña**, e ingréselas nuevamente en el campo **Confirmar contraseña**.

Crear usuario

Esta ventana aparece cuando hace clic en **Crear** en la ficha Nombre de usuario/contraseña local de la ventana Usuarios y contraseñas. Utilícela para especificar un nombre de usuario, contraseña y un nivel de privilegios asociado.

Las opciones disponibles varían, dependiendo del dispositivo que se esté configurando.

Siga estos pasos:

PASO 1 En el campo **Nombre de usuario**, introduzca el nombre que el usuario usará para acceder a Configuration Assistant.

PASO 2 En el campo **Contraseña**, especifique la contraseña que usará el usuario. La entrada está cifrada.

PASO 3 Especifique la contraseña de vista en el campo **Confirmar Contraseña**.

PASO 4 De la lista Nivel de privilegio, seleccione un nivel de privilegio. Dependiendo del dispositivo que se esté configurando, se muestran diferentes opciones de Nivel de privilegios.

Para las plataformas UC500 y otros dispositivos IOS, el Nivel 15 otorga acceso de lectura y escritura; los niveles 1 al 14 otorgan acceso de sólo lectura.

Para los Dispositivos de seguridad SA500, también se puede determinar el Nivel de privilegios como Invitado (para acceso de sólo lectura) y como Usuario de VPN sobre SSL.

Para las cámaras Business Internet Cameras modelos PVC2300 y WVC2300 de Cisco, seleccione uno de los siguientes niveles de privilegios:

- **Admin** - Permite que el usuario administre y controle la cámara y el vídeo.
- **Monitor** — Permite que el usuario controle el vídeo de la cámara (paneo e inclinación manual, paso de visión diurna a nocturna y activar los puertos de salida). Los usuarios de la cámara agregados por medio del Asistente de configuración de monitor de vídeo reciben privilegios de Monitor.
- **Visualizador** — Permite que el usuario vea el vídeo desde la cámara utilizando un explorador de Internet, teléfono IP u otra aplicación.

PASO 5 Haga clic en **Aceptar**. Cuando vuelve a la ventana Usuarios y contraseñas, verá una nueva entrada en la ficha Nombre de usuario/Contraseña local.

Modificar contraseña de usuario

Esta ventana aparece cuando selecciona una entrada y haga clic en **Modificar** en la ficha Nombre de usuario/Contraseña local de la ventana Usuarios y contraseñas. Utilícela para modificar la contraseña y el nivel de privilegio asociado con un nombre de usuario.

Siga estos pasos:

PASO 1 Si desea cambiar la contraseña, introduzca una contraseña distinta en el campo **Contraseña**. La entrada está cifrada y aparece como asteriscos.

PASO 2 Especifique la contraseña de vista en el campo **Confirmar Contraseña**.

PASO 3 Si desea cambiar el nivel de privilegio, seleccione un nivel de privilegio distinto de la lista Nivel de privilegio.

PASO 4 Haga clic en **Aceptar**.

Modificar habilitar contraseña

Esta ventana aparece cuando selecciona una contraseña y haga clic en **Modificar** en la ficha Activar contraseña de la ventana Usuarios y contraseñas. Utilícela para modificar la contraseña para el nivel de privilegio asociado.

Siga estos pasos:

PASO 1 En el campo **Contraseña**, introduzca una contraseña diferente para el nivel de privilegio indicado. Su entrada está cifrada y aparece como estrellas.

PASO 2 Especifique la contraseña de vista en el campo **Confirmar Contraseña**.

PASO 3 Haga clic en **Aceptar**.

Acceso remoto a dispositivos (Telnet)

El acceso remoto a través de Telnet siempre está activado, ya que CCA no funcionará adecuadamente sin acceso a Telnet. La ventana Acceso al dispositivo que se incluía en anteriores versiones de CCA se ha eliminado, y CCA ya no usa SSH.

SNMP

Para configurar SNMP (Protocolo de administración de redes simples), seleccione **Configurar** > **Propiedades del dispositivo** > **Administración de SNMP**.

Visión general

La administración de SNMP incluye las siguientes tareas:

- Activar o desactivar SNMP en un switch autónomo
- Configuración de opciones del sistema
- Agregar y eliminar cadenas de comunidad
- Cómo agregar y eliminar administradores de interrupciones
- Cómo crear vistas de objetos MIB a los que tengan acceso grupos de usuarios
- Cómo asociar vistas a los grupos que tienen acceso a ellas
- Cómo asociar grupos con los usuarios que pertenecen a ellos

Procedimientos

La ventana tiene estas fichas:

- **Opciones del sistema**, para asignar la información administrativa a un dispositivo para poder identificarlo.
- **Cadenas de comunidad**, para agregar y eliminar cadenas de comunidad
- **Administradores de interrupciones**, para agregar y eliminar administradores de interrupciones
- **Filtro (Switches de la serie ESW500)**, para crear conjuntos de interrupciones que pueden enviarse a un administrador de interrupciones (sólo switches de la serie ESW500 de Cisco)

- **Vistas**, para crear vistas de objetos MIB a los que tengan acceso grupos de usuarios
- **Grupos**, para asociar vistas a los grupos que tienen acceso a ellas
- **Usuarios**, para asociar grupos con los usuarios que pertenecen a ellos

Las opciones de configuración de SNMP y de fichas disponibles varían entre los dispositivos. No todos los dispositivos admiten todas estas opciones de configuración de SNMP por medio de CCA.

Comience haciendo lo siguiente:

- Seleccione un dispositivo de la lista **Nombre de host**. Las fichas y sus configuraciones se aplican al dispositivo seleccionado. Las fichas **Vistas**, **Grupos**, y **Usuarios** sólo pueden visualizarse si el dispositivo admite SNMP Versión 3 ó superior.
- Asegúrese que está marcado **Activar SNMP**.

Cuando haya terminado de introducir la configuración en las fichas, haga clic en **Aceptar**.

Opciones del sistema

Aunque SNMP permite un máximo de 255 caracteres para cada campo de la ficha, Configuration Assistant reduce esta información y la transforma en segmentos más cortos. Por este motivo, recomendamos abreviar los datos. Consulte los pasos individuales en el siguiente procedimiento para pautas.

Para asignar opciones del sistema:

PASO 1 En el campo **Ubicación del sistema**, indique la ubicación física del dispositivo. La longitud máxima de una entrada en el campo **Ubicación del sistema** es 129 caracteres.

PASO 2 En el campo **Contacto del sistema**, especifique el nombre u orgarnización responsable del dispositivo. La longitud máxima de una entrada en el campo **Contacto del sistema** es 129 caracteres.

Cadenas de comunidad

Las cadenas de comunidad sirven como contraseñas para autenticar mensajes SNMP. Cada cadena de comunidad es de sólo lectura (RO), lo que permite que la información de objeto MIB, o de lectura y escritura (RW), que permite que la información de objeto MIB se muestre y modifique.

Las cadenas de la primera comunidad de sólo lectura y la primera lectura y escritura se muestran en la ventana de gestión SNMP. Debido a que son necesarios para el enrutamiento de paquetes SNMP, no deben eliminarse de ningún dispositivo.

Además, la configuración de SNMP puede contener cadenas de comunidad que defina el usuario.

Si su modo de acceso es sólo lectura, no ve cadenas de comunidad en esta lista.

Agregar cadenas de comunidad

El dispositivo seleccionado admite una cantidad ilimitada de cadenas de comunidad de cualquier longitud.

Para agregar una nueva cadena de comunidad a un dispositivo:

PASO 1 En el campo **Nueva cadena**, introduzca una cadena de caracteres.

PASO 2 Seleccione **RO** (sólo lectura) o **RW** (lecutra y escritura) para especificar el tipo de cadena.

PASO 3 Haga clic en **Agregar** para desplazar la nueva cadena de comunidad a la lista de **Cadenas actuales**.

Eliminar cadenas de comunidad

No elimine la primera cadena de comunidad de Sólo lectura ni la de Lectura y escritura. Estas cadenas son necesarias para funciones SNMP.

Para eliminar una cadena de comunidad existente:

PASO 1 En la lista **Configuración actual**, seleccione las cadenas de comunidad que van a eliminarse.

PASO 2 Para eliminar todas las cadenas de comunidad, haga clic en **Seleccionar todo**.

PASO 3 Haga clic en **Eliminar**.

Administradores de interrupciones

Un administrador de interrupciones es una estación de administración que recibe interrupciones, las alertas del sistema que genera un dispositivo. Por defecto, no se define ningún administrador de interrupciones y no se envían interrupciones.

Para activar el dispositivo seleccionado para enviar interrupciones, marque **Activar interrupciones**. Luego, marque las casillas para los tipos de interrupciones que desee activar para cada destino IP.

Para agregar un nuevo administrador de interrupciones:

PASO 1 En el campo **Dirección IP**, introduzca la dirección IP del nuevo administrador de interrupciones.

PASO 2 En el campo **Cadena de comunidad**, introduzca la cadena de comunidad para el nuevo administrador de interrupciones.

PASO 3 En el campo **Puerto UPD**, introduzca el puerto UDP del administrador de interrupciones al cual se deben enviar las interrupciones.

PASO 4 Para enviar todos los tipos de interrupciones al administrador de interrupciones, marque **Enviar todas las interrupciones**. De lo contrario, sólo marque los tipos de interrupciones que desee enviar.

PASO 5 Para ver una descripción de los tipos de interrupciones, consulte la documentación para el dispositivo seleccionado.

PASO 6 *Opcional*. Si se está configurando un administrador de interrupciones para un switch de la serie ESW500, se puede seleccionar un filtro para aplicarlo a este Administrador de interrupciones, si se ha definido uno.

PASO 7 Haga clic en **Agregar** para mover sus selecciones a la lista **Administradores actuales**.

Si su modo de acceso es sólo lectura, no ve administradores de interrupciones y sus cadenas de comunidad en esta lista.

Para eliminar un administrador de interrupciones:

PASO 1 En la lista **Administradores actuales** , seleccione los administradores de interrupciones que van a eliminarse.

PASO 2 Para eliminar todos los administradores de interrupciones existentes, haga clic en **Seleccionar todo**.

PASO 3 Haga clic en **Eliminar**.

Filtro (Switches de la serie ESW500)

La ficha Filtro se aplica sólo a los switches Small Business Pro de la serie ESW500 de Cisco.

Esta ficha permite crear, modificar y eliminar filtros SNMP. Un filtro SNMP define un conjunto de interrupciones que se envían a un administrador de interrupciones. Los filtros que se crean en esta ficha pueden seleccionarse en la ficha Administradores de interrupciones.

Para crear un filtro, siga estos pasos:

PASO 1 Haga clic en **Crear**.

PASO 2 En la ventana Crear un filtro de interrupciones SNMP, especifique un Nombre de filtro descriptivo, de 1 a 30 caracteres (no se permiten espacios). Después de aplicar los cambios, este nombre se muestra en el menú Seleccionar filtro de la ficha Administradores de interrupciones.

PASO 3 Seleccione uno o más OID de la lista Disponibles y utilice los botones **Agregar**, **Eliminar**, y **Seleccionar todo** para desplazar OID desde la lista Disponibles a la lista Seleccionados.

PASO 4 Haga clic en **Aceptar** para cerrar la ventana Crear un filtro de interrupciones SNMP.

PASO 5 En la ventana Administración de SNMP, haga clic en **Aplicar** o **Aceptar**.

Para eliminar un filtro, selecciónelo de la lista y haga clic en **Eliminar**. Sólo se pueden eliminar los filtros que no se están utilizando. Si alguno de los Administradores de interrupciones está utilizando el filtro, se le solicitará quitar el filtro del Administrador de interrupciones antes de poder eliminarlo.

Para modificar un filtro, selecciónelo y haga clic en **Modificar**.

Crear o Modificar filtro SNMP (serie ESW500)

Esta ventana aparece cuando se seleccione **Crear** o **Modificar** en la ficha Filtro de la ventana Administración de SNMP para los switches de la serie ESW500 de Cisco.

En esta ventana, se puede crear o modificar filtros SNMP. Un filtro SNMP define un conjunto de interrupciones que se envían a un administrador de interrupciones. Los filtros que se crean en esta ventana pueden seleccionarse en la ficha Administradores de interrupciones de la ventana Administración de SNMP.

Para crear o modificar un filtro SNMP, siga estos pasos:

PASO 1 Especifique un **Nombre de filtro** descriptivo, de 1 a 30 caracteres (no se admiten espacios). Después de aplicar los cambios, este nombre se muestra en el menú Seleccionar filtro de la ficha Administradores de interrupciones.

PASO 2 Utilice los botones **Agregar**, **Eliminar** y **Seleccionar todo** todo para mover a las OID entre las listas Disponible y Seleccionado.

PASO 3 Haga clic en **Aceptar**.

Vistas

Esta ficha muestra los nombres de las vistas, recolecciones de objetos MIB a los que los grupos de usuarios pueden tener:

- Acceso de lectura
- Acceso de escritura
- Privilegios de notificación

Para crear una vista y agregar su nombre a esta ficha, haga clic en **Crear**, y utilice la ventana Crear vista SNMP. Consulte **Crear vista de SNMP, página 149**.

Para modificar una vista, selecciónela, haga clic en **Modificar**, y utilice la ventana Modificar vista SNMP.

Para eliminar una vista, selecciónela y haga clic en **Eliminar**.

No es posible eliminar ni modificar la vista **v1default**.

Crear vista de SNMP

Esta ventana aparece cuando se hace clic en **Crear** en la ficha Vistas de la ventana de SNMP.

Para crear una vista SNMP, siga estos pasos:

PASO 1 Especifique un nombre para la vista en el campo **Nombre de la vista**.

PASO 2 Seleccione una o más OID—ID de objetos MIB —de la lista OID. Para seleccionar todas las OID, haga clic en **Seleccionar todas**.

PASO 3 Haga clic en **Agregar** para añadir las OID seleccionadas a la lista OID incluidas. Estas son las OIDs que conformarán la nueva vista. Para devolver las OID a la lista OID, selecciónelas y haga clic en **Eliminar**.

PASO 4 Haga clic en **Aceptar**. El nombre de la vista creada se indica en la ficha Vistas de la ventana SNMP.

Modificar vista SNMP

Esta ventana aparece cuando se selecciona una vista y se hace clic en Modificar en la ficha Vistas de la ventana de SNMP.

Para modificar la vistaSNMP, siga estos pasos:

PASO 1 En la lista OID, seleccione cualquier OID que desee agregar a la vista. Luego, haga clic en **Agregar**.

PASO 2 En la lista OID incluidas , seleccione cualquier OID que desee eliminar de la vista. Luego, haga clic en **Eliminar**.

PASO 3 Haga clic en **Aceptar**.

Grupos

Las columnas de esta ficha tienen los siguientes significados:

Columna	Significado
Grupo	El nombre de un grupo de usuarios
Nivel de seguridad	Indica si se necesita que los usuarios indiquen una contraseña (**Autentificar**) y si la contraseña está cifrada (**Privacidad**)
Leer vista	Es una vista a la que el grupo tiene acceso de lectura
Vista Escribir	Es una vista a la que el grupo tiene acceso de lectura
Vista Notificar	Es una vista a la que el grupo tiene privilegios de notificación

Para crear un grupo y agregar sus atributos a esta ficha, haga clic en **Crear**, y utilice la ventana Crear grupo SNMP. Consulte **Crear grupo SNMP, página 150**.

Para modificar un grupo, selecciónelo, haga clic en **Modificar**, y utilice la ventana Modificar grupo SNMP.

Para eliminar un grupo, selecciónelo y haga clic en **Eliminar**.

No es posible eliminar ni modificar el grupo **v1default**.

Crear grupo SNMP

Esta ventana aparece cuando se hace clic en **Crear** en la ficha Grupos de la ventana de SNMP. Utilícela para especificar los atributos de un grupo de usuarios de SNMP.

Para crear un grupo SNMP, siga estos pasos:

PASO 1 En la campo **Nombre de grupo**, especifique un nombre para el nuevo grupo.

Es posible especificar el nombre de un grupo que ya existe, siempre que se seleccione un nivel de seguridad diferente. Un nombre de grupo y un nivel de seguridad únicamente identifican a un grupo.

PASO 2 Seleccione un nivel de seguridad de la lista **Nivel de seguridad**.

- No Autenticar significa que no se necesita autenticar el paquete.
- Autenticar significa que se necesita autenticar el paquete.
- Privacidad significa que se necesita cifrar el paquete. Esta opción sólo está acticada si está instalado una imagen de software de cifrado.

PASO 3 *Opcional*: En la lista Vista de Lectura, seleccione una vista a la que el grupo tendrá acceso de lectura.

PASO 4 *Opcional*: En la lista Vista de Escritura, seleccione una vista a la que el grupo tendrá acceso de escritura.

PASO 5 *Opcional*: En la lista Vista Notificar, seleccione una vista con las notificaciones que deben enviarse al grupo.

PASO 6 Haga clic en **Aceptar**. Cuando vuelva a la ventana SNMP, es posible visualizar una nueva entrada en la ficha Grupos.

Modificar grupo SNMP

Esta ventana aparece cuando se selecciona un grupo y se hace clic en **Modificar** en la ficha Grupos de la ventana de SNMP.

A continuación se encuentran los atributos del grupo que se pueden modificar:

- La vista de objetos MIB a la que el grupo tiene acceso de lectura.
- La vista de objetos MIB a la que el grupo tiene acceso de escritura.
- La vista de objetos MIB que se envía al grupo, con notificaciones.

Para obtener mayor información sobre estas opciones de ventanas, consulte el tema **Crear grupo SNMP**.

Haga clic en **Aceptar** cuando termine.

Usuarios

Esta tabla explica lo que contiene cada una de las columnas de la ficha.

Columna	Contenidos
Usuario	Nombres de los usuarios
Grupo	El grupo al que pertenecen los usuarios adyacentes
Algoritmo de autentificación	El tipo de algoritmo que se usa para cifrar la contraseña de autentificación

Para asignar un usuario a un grupo y agregarlo a esta ficha, haga clic en **Crear**, y utilice la ventana Crear usuario SNMP. Consulte **Crear usuario SNMP, página 152**.

Para modificar los atributos de un usuario, incluyendo el grupo al que pertenece el usuario, seleccione la entrada para este usuario, haga clic en **Modificar**, y utilice la ventana Modificar usuario SNMP.

Para eliminar un usuario, seleccione su entrada y haga clic en **Eliminar**.

Crear usuario SNMP

Esta ventana aparece cuando se hace clic en **Crear** en la ficha Usuarios de la ventana de SNMP. Utilícela para especificar los atributos de un usuario SNMP.

Para crear usuarios SNMP, siga estos pasos:

PASO 1 En el campo **Nombre de usuario**, especifique un nombre para el usuario.

PASO 2 En la lista **Nombre de grupos**, seleccione el grupo al que pertenece el usuario. (Primero, se debe definir el grupo en la ficha Grupos).

PASO 3 *Opcional*: En el área Autentificación, realice estas acciones si el usuario necesitará una contraseña de autentificación:

a. Seleccione un algoritmo de autentificación de la lista **Algoritmo de autentificación**.

b. Especifique una contraseña en el campo **Contraseña** para que el usuario la indique al momento de su autentificación.

c. Especifique la contraseña de vista en el campo **Confirmar Contraseña**.

PASO 4 Haga clic en **Aceptar**. Cuando vuelva a la ventana SNMP, es posible visualizar una nueva entrada en la ficha Usuarios.

Modificar usuario SNMP

Esta ventana aparece cuando se selecciona un usuario y se hace clic en Modificar en la ficha Usuarios de la ventana de SNMP.

A continuación se encuentran los atributos del usuario que se pueden modificar:

- El grupo al que pertenece el usuario, seleccionando un nombre de grupo diferente.
- El algoritmo de autentificación, si existe.
- La contraseña de autentificación y la de confirmación, si existen.

Para obtener mayor información sobre estas opciones de ventanas, consulte el tema **Crear usuario SNMP**.

Haga clic en **Aceptar** cuando termine.

5

Configuración de puertos y switch

Esta sección cubre la configuración de puertos y switches. Incluye los siguientes temas:

- **Configuración de puertos de switch**
- **Smartports**
- **VLANs**
- **Reflejo de puertos (switches de la serie ESW500)**
- **Spanning Tree Protocol (switches CE520)**
- **Snooping IGMP (switches CE520)**
- **Direcciones MAC (switches CE520)**
- **Ventana Búsqueda de puertos (switches CE520)**
- **EtherChannels (switches CE520)**

Configuración de puertos de switch

Para configurar puertos de switch:

- Seleccione **Configurar** > **Puertos** > **Configuración de puertos de switch** en la barra de funciones.
- Haga clic en el icono Switchports de la barra de herramientas.

Visión general

Por defecto, todos los puertos en un switch están activados y los parámetros del puerto se definen con valores iniciales. La ventana Configuración de puerto despliega tres valores y le permite cambiarlos.

Algunos tipos de puerto negocian automáticamente los ajustes de configuración. Una diferencia en la negociación automática puede ocurrir bajo estas condiciones:

- Cuando un parámetro dúplex definido manualmente es diferente del definido en el puerto conectado
- Cuando un puerto se configura en Auto-negociación y el puerto asociado se configurar como full-dúplex sin Auto-negociación

El resultado de una diferencia en los puertos Fast Ethernet es un menor desempño o errores en el enlace. En los puertos Gigabit Ethernet, el enlace no se activa y no se informan las estadísticas.

Para corregir las configuraciones del puerto que muestran diferencias, haga una de estas sugerencias:

- Permita que ambos puertos negocien automáticamente tanto la velocidad como el dúplex.
- Defina manualmente los parámetros de velocidad y dúplex para los puertos en ambos extremos de la conexión.

Para conectar un dispositivo Fast Ethernet remoto que no negocie automáticamente, debería definir explícitamente el dúplex en el dispositivo local en un valor que no sea **Auto**. La negociación de velocidad funciona incluso si otro dispositivo no negocia automáticamente.

Para conectarse a un dispositivo Gigabit Ethernet remoto que no negocie, desactive la negociación automática en el dispositivo local y defina los parámetros dúplex y de control de flujo que sean compatibles con el dispositivo remoto.

Procedimientos

Comience al seleccionar un dispositivo de la lista **Nombre del host**. La información sobre los puertos del dispositivo está en estas fichas:

- **Ajustes de la configuración, página 157** que muestra los valores que se pueden configurar y modificar.
- **Estado de operación, página 160** que muestra el estado actual de los puertos.

Para ver un subconjunto de información de cualquier ficha, haga clic en **Filtro** y utilice la ventana Editor de filtro. Consulte **Filtro, página 162**.

Ajustes de la configuración

Esta tabla explica la información sobre esta ficha.

Configuración	Explicación
Descripción	Descripción del puerto. Haga clic en **Describir** en la ventana Configuración de puertos para describir múltiples puertos. No se puede utilizar el caracter ? ni el caracter /. Si seleccionó más de un puerto, este campo no está disponible.
Estado	Configuración para activar o desactivar el puerto, puede ser distinta de la configuración de ejecución. Por ejemplo, si no hay un dispositivo conectado al puerto, éste se puede activar administrativamente con un estado de ejecución de DOWN. Si cambia otros parámetros en un puerto desactivado, éstos no se hacen efectivos hasta que active el puerto. Cuando usted desactiva un puerto, una interrupción *linkdown* se envía a la estación de administración si configuró un administrador de SNMP.
Dúplex	Configuración para dúplex: full duplex, half duplex o auto. La configuración por defecto para los puertos Gigabit Ethernet y GigaStack GBIC es auto. Estos puertos automáticamente asocian la capacidad dúplex de un dispositivo conectado. Para definir un valor dúplex que no sea auto, el valor de la velocidad debe ser distinto a auto. El valor dúplex debe ser auto si la velocidad del puerto está definida en auto y si el puerto puede ejecutar a una velocidad de 1000 Mbps. Las conexiones de pila GigaStack GBIC operan en el modo half-duplex. Las conexiones del puerto GigaStack GBIC de punto a punto operan en el modo full-duplex.

Configuración	Explicación
Velocidad	Configuración para los puertos 10/100-Mbps y 10/100/1000-Mbps: ▪ *10* (los puertos ejecutan a una velocidad forzada de 10 Mbps) ▪ *100* (los puertos ejecutan a una velocidad forzada de 100 Mbps) ▪ *1000* (los puertos ejecutan a una velocidad forzada de 1000 Mbps) ▪ *auto* (los puertos negocian automáticamente y anuncian las velocidades disponibles) ▪ *auto 10* (los puertos negocian automáticamente y anuncian velocidades de 10 Mbps para el otro extremo del enlace) No disponible en los switches de la serie ESW 500. ▪ *auto 100* (los puertos negocian automáticamente y anuncian velocidades de 100 Mbps para el otro extremo del enlace) No disponible en los switches de la serie ESW 500. ▪ *auto 100 1000* (los puertos negocian automáticamente y anuncian velocidades de 100 y 1000 Mbps para el otro extremo del enlace) ▪ *auto 10 1000* (los puertos negocian automáticamente y anuncian velocidades de 10 y 1000 Mbps para el otro extremo del enlace) ▪ *auto 1000* (los puertos negocian automáticamente y anuncian velocidades de 1000 Mbps para el otro extremo del enlace) ▪ *auto 10 100* (los puertos negocian automáticamente y anuncian velocidades de 10 y 100 Mbps para el otro extremo del enlace) ▪ *auto 10.100 1000* (los puertos negocian automáticamente y anuncian velocidades de 10, 100 y 1000 Mbps para el otro extremo del enlace) La configuración por defecto para los puertos 10/100- y 10/100/1000-Mbps es auto. Los puertos Ethernet pueden asociar automáticamente la velocidad de transmisión de un dispositivo conectado. **NOTA** No se puede modificar la configuración de velocidad de estos puertos:

Configuración	Explicación
Energía	Esta configuración se aplica a un sólo puerto en un switch Catalys Express de la serie 500 PoE o ESW500. Seleccione **auto** si quiere que el puerto detecte un dispositivo de energía y le suministre energía. De lo contrario, seleccione **nunca**.
Auto MDIX	Sólo switches de la serie ESW500. Muestra el esado de la Interfaz dependiente del medio (MDI)/ Interfaz dependiente del medio con cruce (MDIX) en un puerto del switch ESW500. Los hubs y los switches se cablean deliberadamente en forma opuesta a como se cablean las estaciones finales, para que cuando un hub o switch está conectado a una estación final, un cable Ethernet recto puede usarse y los pares coincidan adecuadamente. Cuando dos hubs o switches se conectan entre sí, o dos estaciones finales están conectadas entre sí, se usa un cable de cruce para asegurar que se conecten los pares correctos. Realice una de las siguientes configuraciones: ▪ **Auto**. Se usa para detectar automáticamente el tipo de cable. Ésta es la configuración predeterminada. ▪ **MDIX**. Se usa para hubs y switches. ▪ **MDI**. Se usa para estaciones finales.

Para modificar la configuración de puertos un puerto cada vez, haga clic en la celda correspondiente al puerto que desea modificar.

Para modificar la configuración de uno o más puertos:

PASO 1 Seleccione los puertos en la columna Interfaz. Mantega pulsada la tecla **Ctrl** y realice su selección o mantenga presionada la tecla **Shift** y seleccione el primer y último puerto en un intervalo.

PASO 2 Haga clic en **Modificar** para desplegar la ventana Modificar configuración del puerto. Consulte **Modificar configuraciÃ³n de puerto, página 161**.

PASO 3 Complete los campos en la ventana Modificar configuración de puertos.

PASO 4 Haga clic en **Aceptar** para cerrar la ventana y volver a la ventana Configuración de puertos.

Estado de operación

Esta tabla explica la información de sólo lectura sobre esta ficha.

Columna	Explicación
Interfaz	Identifica al puerto: Fast Ethernet, Gigabit Ethernet o FDDI, el número de ranura o módulo (0, 1 ó 2) y el número de puerto.
Descripción	La descripción de la interfaz.
Enlace ethernet	Estado del puerto. El estado de un puerto puede ser activado, desactivado, o desactivado administrativamente.
Dúplex	Estado dúplex del puerto (híbrido, medio, completo). Muestra el modo dúplex del puerto. Para los switches de la serie ESW500, Completo (Full) indica que la interfaz admite la transmisión entre el dispositivo y el cliente en ambas direcciones en forma simultánea y Medio (Half) indica que la interfaz admite la transmisión entre el dispositivo y el cliente en sólo una dirección a la vez.
Velocidad	La velocidad del puerto. Para los puertos Gigabit Ethernet, este campo es de sólo lectura y muestra *1000* (1000 Mbps).
Estado	Muestra si la energía en la línea está siendo suministrada a un dispositivo conectado.
Presupuesto	Cantidad de energía asignada al dispositivo conectado.
Dispositivo	Muestra el tipo de dispositivo que está recibiendo energía en la línea desde la interfaz.
Clase	La clasificación IEEE del dispositivo energizado. Muchos dispositivos energizados no requieren todos los 15,4 Watts de energía disponible con PoE. Las clases de energía varían entre 0 y 4. El valor por defecto es 0. La energía asignada para el switch depende de la clase IEEE.

Modificar configuraciÃ³n de puerto

La ventana Modificar configuración de puertos aparece cuando se seleccionan múltiples puertos en la ventana Configuración de puertos del switch.

Especifique o seleccione valores para los puertos que se van a modificar. Consulte **Ajustes de la configuración, página 157** para conocer las descripciones de lo que se debe especificar.

Si selecciona múltiples puertos y especifica un ajuste de configuración que no es válido para el puerto seleccionado, la configuración actual permanece sin cambios. Por ejemplo, si selecciona un puerto 10BaseT Ethernet, Fast Ethernet y Gigabit y luego selecciona una velocidad de 100 Mbps, el puerto 10BaseT Ethernet permanece en 10 Mbps y el puerto Gigabit permanece en 1000 Mbps.

Haga clic en **Aceptar** para cerrar la ventana. Las modificaciones aparecen en la ventana Configuración del puerto.

Para obtener más información, consulte estos temas:

- **Ajustes de la configuración, página 157**
- **Estado de operación, página 160**

Modificar descripciones del puerto

Para agregar o modificar las descripciones del puerto:

Seleccione uno o más puertos. Si selecciona un puerto, haga clic en la celda de la columna **Descripción** para el puerto que desea describir. Introduzca texto donde se ve el cursor parpadeante.

Si selecciona más de un puerto:

PASO 1 Haga clic en **Describir** para desplegar la ventana Descripción básica del puerto.

PASO 2 Completar la configuración de la ventana. Desde la ventana Descripción básica del puerto, puede ir a la ventana Descripción avanzada del puerto para especificar el aumento automático de hasta tres (3) descriptores.

PASO 3 Haga clic en **Aceptar** para cerrar la ventana.

Filtro

La ventana Filtro aparece cuando hace clic en **Filtro** en una ventana o asistente de Configuration Assistant que contiene una tabla. Los nombres de columnas en la tabla se transforman en los nombres de campos en esta ventana. Introduzca criterios de selección en los campos para filtrar las filas de la tabla y dejar sólo aquellas que le interesan.

Siga estos pasos:

PASO 1 Deja un campo en blanco si no desea filtrar su correspondiente columna de la tabla, es decir, si usted no tiene criterios de selección de la columna.

PASO 2 Para utilizar un campo con una lista desplegable, seleccione un elemento para que Configuration Assistant compare entradas en la columna correspondiente.

PASO 3 Para utilizar un campo de entrada de texto, introduzca caracteres para que Configuration Assistant compare entradas en la columna correspondiente. Utilice una estrella (*) como un marcador de posición para una cadena de caracteres de cualquier longitud. Utilice un signo de interrogación (?) como un marcador de posición para cualquier carácter individual. Para hacer coincidir una cadena sin importar los caracteres que la anteceden o siguen, introduzca **cadena**.

Ejemplos

- Para ver sólo las interfaces en la ventana Actualización de software LRE que están activadas para una actualización, seleccione **activar** en el campo **Actualizar** de la ventana Editor de filtro que sirve la ventana Actualización de software LRE.
- Para ver sólo las descripciones en la ventana Configuración de puertos que contiene la cadena 1234, introduzca ***1234***en el campo **Descripción** de la ventana Editor de filtro que sirve la ventana Configuración de puertos.

PASO 4 Haga clic en **Aceptar**. Usted vuelve a la ventana o asistente de Configuration Assistant que estaba utilizando y ve el subconjunto de información que solicitó.

Smartports

Para configurar las conexiones de puertos, a éstos se les aplican perfiles. Para abrir la ventana Smartports y acceder a esta configuración:

- Seleccione **Configurar** > **Conmutación** > **Smartports** en la barra de funciones.
- Haga clic en el icono Smartports de la barra de herramientas.
- Haga clic en **Resolver** en la ventana Notificación de evento para aplicar el perfil Smartports.

Visión general

Smartports es una solución que le ayuda a configurar las funciones esenciales de seguridad, disponibilidad y gestionabilidad de las conexiones de puertos de su red.

La ventana Smartports muestra los paneles frontales de los dispositivos; usted selecciona los puertos y les aplica perfiles. Usted puede configurar una conexión de puerto a estos dispositivos:

Dispositivo	Comentarios
Escritorio	Un host de extremo interno con acceso a Internet y a las subredes internas de una organización.
Teléfono IP	Un host final, como una PC, puede conectarse en cascada a un teléfono IP.
Switch	Una conexión de switch a switch.
Router	An router de acceso o una plataforma UC 500.
Punto de acceso	Un punto de acceso puede conectarse a host finales móviles. Según la configuración del punto de acceso, los hosts finales móviles pueden ser hosts finales invitados o de escritorio.

Procedimientos

Esta ventana muestra una vista del panel frontal de los dispositivos de su red. Si hay un puerto conectado a un dispositivo y se le ha aplicado un perfil, verá el icono para el dispositivo conectado sobre el puerto. Cuando desplace el cursor del ratón sobre el icono, Configuration Assistant indentificará el tipo de dispositivo que está conectado.

Para aplicar perfiles a otros puertos conectados o para conectar un perfil mal aplicado (como lo indica el icono), realice una de las siguientes acciones:

- Haga clic en **Sugerir**. Los iconos de los dispositivos conectados parpadean sobre los puertos, y aparece la ventana Smartports sugeridos. Sugiere los perfiles que deberían aplicarse a los puertos. Consulte **Smartports sugeridos, página 166**.
- Seleccione un puerto y haga clic en **Modificar**. Aparece la ventana Modificar perfiles de puertos. También se puede utilizar esta ventana para eliminar o aplicar los perfiles de Smartports que no tengan conexiones de dispositivos. Consulte **Modificar perfiles de puerto, página 164**.

Notas:

- Para seleccionar múltiples puertos, mantenga presionada la tecla **CTRL** y haga clic en los puertos que desea. También puede *unir* puertos al mantener presionado un botón del mouse y dibujar un rectángulo alrededor de un grupo de puertos. Mantenga presionada la tecla **CTRL** para unir grupos separados de puertos.
- Cuando usted utiliza CCA para aplicar un perfil, éste reemplaza a los perfiles aplicados anteriormente.

Cuando vuelva a la ventana Smartports, verá los iconos de dispositivos sobre los puertos para los que se seleccionaron perfiles. Si le pidió a CCA que eliminara perfiles, desaparecen los iconos que aparecían previamente.

Para ver detalles acerca de los puertos configurados, haga clic en **Detalles** para abrir la ventana Detalles de perfiles de puerto. Consulte **Smartports sugeridos, página 166**.

Para obtener más información, consulte estos temas:

- **Modificar perfiles de puerto, página 164**
- **Detalles del rol de puerto, página 166**
- **Smartports sugeridos, página 166**

Modificar perfiles de puerto

Esta ventana aparece cuando selecciona uno o más puertos en la ficha Configuración de puerto de la ventana Smartports y haga clic en **Modificar**. Si selecciona un puerto, el campo **Interfaz** muestra el nombre del puerto. Si selecciona más de un puerto, el campo **Interfaz** muestra **Múltiple**.

Para aplicar un rol a los puertos seleccionados, siga estos pasos:

de la lista **Rol**, seleccione un rol que corresponda al dispositivo que quiere conectar.

Dispositivo	Comentarios
Escritorio	Un host de extremo interno con acceso a Internet y a las subredes internas de una organización.
Teléfono IP + Escritorio	Un host final, como una PC, puede conectarse en cascada a un teléfono IP.
Switch	Una conexión de switch a switch.
Router	An router de acceso o una plataforma UC500.
Punto de acceso	Un punto de acceso puede conectarse a host finales móviles. Según la configuración del punto de acceso, los hosts finales móviles pueden ser hosts finales invitados o de escritorio.

Si seleccionó un puerto 10-Gigabit Ethernet, sólo aparecen disponibles las opciones **Switch** y **Router**.

Complete la sección **Atributos** según el rol que seleccionó.

Si seleccionó...	Siga estos pasos...
Escritorio	Introduzca el número de una VLAN en el campo **VLAN de acceso**. Ésta es la VLAN que enviará datos entre el puerto y el escritorio.
IP Phone+Desktop	▪ En el campo **VLAN de acceso**, seleccione la VLAN de datos (por lo general, VLAN1). Ésta es la VLAN que enviará paquetes de datos hacia y desde el puerto. ▪ En el campo **VLAN de voz**, seleccione la VLAN de voz (por lo general, cisco-voice). Ésta es la VLAN que enviará paquetes de voz hacia y desde el puerto.
Router o punto de acceso	Especifique el número de la VLAN nativa en el campo **VLAN nativa**. El puerto será configurado como puerto troncal y la VLAN nativa enviará tráfico no etiquetado.

Switch	Especifique el número de la VLAN nativa en el campo **VLAN nativa**. El puerto será configurado como puerto troncal y la VLAN nativa enviará tráfico no etiquetado. Marque la casilla **Permitir sólo VLAN internas** para permitir todo el tráfico para todas las VLAN, excepto las VLAN Guest y DMZ. Si no está marcada la casilla, se permite el tráfico para todas las VLAN. Si no hay una VLAN Guest ni DMZ configurada, esta casilla queda desactivada. Se debe configurar una VLAN Guest o DMZ para activar esta casilla.

Para eliminar un rol desde los puertos seleccionados, elija **ninguno** de la lista **Rol**. El puerto se restablece a los valores por defecto de fábrica.

Haga clic en **Aceptar** cuando termine con esta ventana. Vuelve la ventana Smartports.

Detalles del rol de puerto

Esta ventana aparece cuando se hace clic en **Detalles** en la ficha Configuración de puerto de la ventana Smartports.

Si usted seleccionó los puertos antes de hacer clic en **Detalles**, se ven encabezados expandidos para los dispositivos con los puertos seleccionados. Si usted no seleccionó puertos, se verán encabezados expandidos para todos los dispositivos en la ventana Smartports.

Bajo los encabezados del dispositivo están los encabezados ampliados del puerto y bajo éstos están los detalles del perfil. Si se aplica un perfil a un puerto, usted verá el tipo de perfil y la información de configuración relacionada. Si no se aplica el perfil, usted verá ninguno.

Haga clic en **Aceptar** cuando termine con esta ventana.

Smartports sugeridos

Esta ventana aparece cuando realiza una de estas acciones:

- Hace clic en **Sugerir** en la ventana Smartports.
- Haga clic en **Resolver** en la ventana Notificación de evento para aplicar el perfil Smartports.

Use la ventana para:

- Configure las VLAN para los perfiles de puertos sugeridos para teléfonos IP, switches, routers, o puntos de acceso.
- Corrija los perfiles aplicados erróneamente.

Para asignar un perfil a un puerto:

PASO 1 Acepte el perfil en la columna Perfil sugerido.

Notas:

- Algunas veces, Configuration Assistant detecta el tipo de dispositivo conectado como un switch cuando el tipo de dispositivo real es un router y viceversa. Modifique el perfil del puerto si el tipo de deispositivo sugerido es incorrecto.
- Si el dispositivo conectado es un punto de acceso, se puede aceptar el perfil de **Punto de acceso** sugerido o modificar el perfil del puerto.
- Configuration Assistant no puede detectar un switch ni un Sniffer que esté conectado a un puerto de switch de Cisco Express 500. Por ende, no se visualizarán perfiles sugeridos para estas conexiones.

PASO 2 Seleccione una VLAN (dos VLAN para teléfonos IP). Esta tabla muestra que selecciones de VLAN se necesitan para cada tipo de conexión de dispositivo.

Para conexiones a	Seleccione...
Un teléfono IP + escritorio	Una VLAN de acceso y una VLAN de voz
Escritorio	Una VLAN de acceso
Un switch	La VLAN nativa
Un router	La VLAN nativa
Un punto de acceso	La VLAN nativa

Las VLAN que seleccione deben corresponder a las conexiones que esté configurando. Si una VLAN que necesita no está en la lista, entonces no existe. Cierre esta ventana y la de Smartports, utilice la ventana VLAN para crear la VLAN y luego utilice la función Smartports de nuevo.

PASO 3 Haga clic en **Aceptar** cuando termine.

PASO 4 En la ventana Smartports, haga clic en **Aceptar** para aplicar los perfiles para los que se configuraron las VLAN.

VLANs

Esta ventana aparece cuando se selecciona **Configurar** > **Conmutación** > **VLANs** en la barra de funciones.

Cuando se selecciona un dispositivo de la lista **Nombre del host** , se verá la siguiente información para cada VLAN:

- ID de VLAN
- Nombre de VLAN
- Dirección IP, subred y máscara de subred
- VLAN de voz por defecto (indicada por una marca de verificación en griego)

Si los dispositivos sincronizados con la VLAN, tales como un UC500, switches de la serie ESW500 y switches de la serie Catalyst Express CE520 son parte del sitio de clientes, el selector del dispositivo **Nombre del host** muestra el valor **All UC5xx/CE/ESW**.

Consulte las siguientes secciones para obtener mayor información sobre las VLAN y la configuración de VLAN:

- **Visión general**
- **Notas**
- **Procedimientos**

Visión general

Se puede crear las VLAN para los siguientes dispositivos:

- Todos los dispositivos UC500
- Todos los dispositivos SR500
- Todos los dispositivos C8xx

Una VLAN (LAN Virtual) es una red con switches que está segmentada lógicamente por función, equipo de proyectos, o aplicaciones, sin considerar las ubicaciones físicas de los usuarios. Las VLAN tienen los mismos atributos que las LAN físicas, pero se pueden agrupar las estaciones de los extremos, incluso, si ellas no están físicamente ubicadas en el mismo segmento de la LAN. Cualquier puerto de switch puede pertenecer a una VLAN, y los paquetes de unidifusión, difusión y multidifusión se envía y dirigen sólo a las estaciones de extremo de la VLAN.

Las VLANs definen los dominios de transmisión en una red de nivel 2. Un dominio de transmisión es el conjunto de todos los dispositivos que recibirán tramas de transmisión que se originen en cualquier dispositivo dentro de dicho conjunto. Típicamente los dominios de transmisión se unen por medio de routers, ya que éstos no envían tramas de transmisión. Los switches de nivel 2 crear dominios de transmisión basados en la configuración del switch. Los switches son puentes con múltiples puertos que permiten crear múltiples dominios de transmisión. Cada dominio de transmisión es similar a un puente virtual distinto dentro de un switch.

Es posible definir uno o más puentes virtuales dentro de un switch. Todo puente virtual que se cree en el switch define un nuevo dominio de transmisión (VLAN). El tráfico no puede pasar directamente a otra VLAN (entre dominios de transmisión) dentro del switch ni entre dos switches. Para interconectar dos VLANs diferentes, se debe utilizar routers o switches de nivel 3.

Por defecto, los switches se configuran con una sola VLAN, VLAN1. Si desea crear VLAN adicionales, esto puede hacerse en la ventana VLAN. También es posible utilizar esta ventana para cambiar el nombre de una VLAN o para eliminarla.

Cuando se crea, modifica o elimina una VLAN en un switch o en una plataforma de comunicaciones unificadas de la serie 500, su acción se duplican automáticamente en todos los dispositivos de estos tipos de su sitio de cliente. La duplicación preserva la congruencia de la VLAN entre los dispositivos. Si se agrega un dispositivo al sitio que ya tenga una VLAN asociada a él, se produce un conflicto de VLAN con los dispositivos que no tengan esta asociación a VLAN. Cuando ello sucede, se le solicitará utilizar la ventana Sincronización de VLAN para restablecer la congruencia de la VLAN. Consulte **Sincronización de VLAN, página 172**.

Notas

Las siguientes notas se aplican a la creación y modificación de VLAN:

- Es posible asignar hasta 15 VLAN con un dispositivo. Todos los dispositivos están asociados, por defecto, a la VLAN 1.
- Sólo el nombre y la ID de la VLAN se sincronizan con los switches ESW500 y CE520.
- En una implementación de múltiples sitios, sólo puede configurarse en el UC500 local. Los cambios en la VLAN realizados en el UC500 local no se aplican a los otros UC500 en una implementación de múltiples sitios y sólo se sincronizan los dispositivos locales.

Procedimientos

Para crear una VLAN, seleccione un **Nombre de host**, haga clic en **Crear**, y complete la configuración en la ventana Crear VLAN. Consulte **Crear VLAN, página 171**.

Para cambiar el nombre, dirección IP, subred o máscara de subred de una VLAN, seleccione la VLAN en esta ventana y haga clic en **Modificar**. Consulte **Sincronización de VLAN, página 172**. VLAN 1 está reservada para CCA, así que no se puede modificar su nombre ni su ID de VLAN.

Para eliminar una VLAN, selecciónela y haga clic en **Eliminar**.

Cuando haya finalizado de hacer cambios, haga clic en **Aceptar** o **Aplicar**.

Para obtener más información, consulte estos temas:

- **Crear VLAN, página 171**
- **Sincronización de VLAN, página 172**

Crear VLAN

Esta ventana aparece cuando hace clic en **Crear** en la ventana VLAN (**Configurar** > **Conmutación** > **VLANs**).

Para crear una VLAN, complete los campos de la ventana Crear VLAN como se describe a continuación y haga clic en **Aceptar**.

Una vez que se ha creado la nueva VLAN, se puede seleccionar **Configurar** > **Enrutamiento** > **Servidor DHCP** para crear un conjunto DHCP, intervalos de exclusión DHCP y asociadiones DHCP, si es necesario.

Configuración	Descripción
ID de VLAN	Especifique la ID de la VLAN. Utilice una ID del intervalo entre 2 y 1000. No especifique 1; esta ID está reservada par la VLAN de datos por defecto.
Nombre de VLAN	El nombre por defecto es VLANxxxx, donde xxxx representa cuatro dígitos (incluyendo los ceros de encabezado) iguales al número de la ID de la VLAN. Puede usar este valor o escribir un nombre de VLAN a partir de 1 hasta 32 caracteres. El nombre de la VLAN debe ser único. La VLAN de voz por defecto debe llamarse Cisco-Voice. El nombre Cisco Voice para la VLAN lo reserva CCA.
Hacer la VLAN de voz por defecto	Cuando se marca esta opción, esta VLAN se usa para la VLAN de voz por defecto. La VLAN de voz por defecto es VLAN100.
Dirección IP	Escriba la dirección IP para esta VLAN. Si se modifica la dirección IP para las VLAN de voz o datos por defecto, también se modifican sus correspondientes firewall, y conjuntos NAT y DHCP. La dirección IP no puede ser un duplicado ni una sobreposición de otras direcciones IP de las interfaces existentes.
Subred	Escriba la subred para esta VLAN.
Máscara de subred	Escriba la máscara de subred para esta VLAN o seleccione una de la lista desplegable.

Sincronización de VLAN

Los dispositivos de su comunidad deben tener configuradas las mismas VLAN. Si no, CCA muestra un icono del evento en la barra de estado y registra el conflicto en la ventana NotificaciÃ³n de eventos. Cuando se reconoce el evento en esa ventana y se hace clic en **Resolver**, aparece la ventana Sincronización de VLAN. En esta ventana, se resuelven los conflictos de VLAN.

Esta tabla explica las columnas de la ventana.

Columna	Explicación
ID de VLAN	Las ID de las VLANs que tienen un conflicto.
Conflicto	Una descripción del conflicto: ▪ No existe: La VLAN no está configurada en todos los dispositivos. ▪ Existe con un nombre diferente: Las ID de VLAN coinciden en todos los dispositivos, pero los nombres de las VLAN no coinciden en todos los dispositivos.
Acción de resolución	Lista de acciones desplegable que resolverán el conflicto. Podrá seleccionar la acción que mejor se adapte a sus necesidades.

Cuando se haya seleccionado las acciones para cada conflicto de VLAN, haga clic en **Resolver**. Podrá ver que sus acciones se reflejan en la ventana VLAN abierta.

No se puede hacer clic en **Resolver** hasta que se seleccione una acción para cada conflicto de VLAN.

Haga clic en **Aplicar** en la ventana VLAN para guardar las acciones y realizar otras tareas, o haga clic en **Aceptar** para guardarlos y cerrar la ventana.

Reflejo de puertos (switches de la serie ESW500)

Para configurar un reflejo de puertos en switches de la serie ESW500 de Cisco, seleccione **Configurar** > **Puertos** > **Reflejo de puertos** en la barra de funciones.

Visión general

El reflejo de puertos monitorea y refleja el tráfico de la red enviando copias de los paquetes entrantes y salientes desde un puerto a un puerto de monitoreo. Puede usarse la función reflejo de puertos como herramienta de diagnóstico y/o como función de depuración. También permite el monitoreo del desempeño del switch.

Los administradores de la red configuran el reflejo de puertos seleccionando un puerto de destino para copiar todos los paquetes, y hasta 8 puertos de origen diferentes desde donde se copiarán los paquetes.

Pautas importantes

- Antes que se puede configurar la función reflejo de puertos en los switches de la serie ESW500, debe configurarse el perfil de Smartport para el Puerto de destino como **Otro**.
- No utilice los puertos de los switches ni los puertos de enlace para espejos de puertos.
- No se puede utilizar el mismo puerto tanto como destino ni como puerto de origen.
- Los puertos de origen y destino deben residir en el mismo switch.

Procedimientos

Para configurar reflejo de puertos, determine la configuración como se describe a continuación, y luego, haga clic en Aceptar.

Configuración	Descripción
Puerto de destino	Define el puerto en el que se refleja el tráfico del puerto de origen.
Puerto de origen	Define el puerto desde el que se va a analizar el tráfico. Puede seleccionarse hasta 8 puertos como puertos de origen.
Tipo	Indica la configuración del modo del puerto para la función reflejo de puertos. Los valores del campo posibles son: ▪ **Sólo recibir**. Define la función de espero de puertos para recibir tráfico sólo en el puerto seleccionado. ▪ **Sólo transmitir**. Define la función de reflejo de puertos para los puertos de transmisión. Éste es el valor predeterminado. ▪ **Transmitir y recibir**. Define la función de reflejo de puertos tanto en los puertos receptores como en los transmisores.

Spanning Tree Protocol (switches CE520)

Para configurar Spanning Tree Protocol (STP) para los switches CE520, seleccione **Configurar** > **Conmutación** > **STP**.

Visión general

Spanning Tree Protocol (STP) es una técnica estandarizada para mantener una red de puentes o switches múltiples. Cuando cambia la topología de la red, STP evita que se generen loops al hacer que los puertos estén en estado de envío o bloqueo, y reconfigura los puentes y switches en forma transparente. Cada VLAN se trata como una red separada y se aplica una instancia separada de STP a cada una.

Este switch admite el protocolo PVST+, de acuerdo con las extensiones protegisdas de Cisco y del estándar IEEE 802.1D.

Los parámetros de STP se configuran para cada VLAN. Para cada instancia de spanning-tree, usted puede configurar un conjunto de opciones globales y un conjunto de parámetros de puerto. El switch admite hasta 32 instancias de spanning-tree.

Usted puede configurar STP en estas formas:

- Cambie el estado STP para **desactivarlo** (o **activarlo**) en una o más VLAN.
- Cambiar parámetros de spanning-tree para el switch raíz.

Procedimientos

La ventana STP tiene estas fichas:

- **Estado de STP** para activar o desactivar STP en una o más VLAN
- **Raíces actuales** ver la configuración raíz actual de spanning-tree

Comience seleccionando un switch de la lista **Nombre de host**. La información de las fichas se aplica al switch seleccionado.

Para ver un subconjunto de información de puertos en las fichas, haga clic en **Filtro** y utilice la ventana Editor de filtro (consulte **Filtro, página 162**). Haga clic en **Actualizar** para encuestar el dispositivo y desplegar los datos más recientes.

Cuando termine de configurar STP, haga clic en **Aceptar**.

Estado de STP

Esta ficha muestra si STP está activado para cada VLAN del switch. STP está activado por defecto. Sin embargo, al desactivar STP, es posible evitar el retraso de 30 segundos en el envío de paquetes desde un puerto, cuando se reconfigura un switch.

Este switch sólo admite el protocolo PVST+, que se representa por medio de **pvst** en la lista **Modo Spanning-Tree** .

IMPORTANTE Desactive a STP sólo si está seguro que no existen bucles en la topología de su red. Si se desactiva STP y existen bucles en la topología, se reduce el rendimiento de la red al haber un exceso de tráfico y una duplicación indefinida de paquetes.

Para activar o desactivar STP:

PASO 1 En la columna **ID de VLAN**, seleccione una o más VLAN en las que desee desactivar o activar STP.

PASO 2 En la columna **Estado de spanning-tree**, seleccione **activar** en la lista desplegable para activar a STP para cda VLAN que haya seleccionado.

Seleccione **desactivar** para desactivar STP para cada VLAN que haya seleccionado.

Raíces actuales

Para cada VLAN, la ficha **Raíz actual** (una ficha de sólo lectura) muestra la configuración de STP del switch de raíz actual. Esta configuración, que podría definirse en otro switch, define los parámetros que entran en efecto cuando el switch está actuando como la raíz de la VLAN.

Esta configuración se describe en la tabla a continuación.

Campo	Descripción
ID de VLAN	La VLAN a la que se aplica esta configuración cuando el swtich actúaa como la raíz.
Dirección MAC	La dirección MAC del switch de raíz.

Campo	Descripción
Prioridad	Identifica el puente de raíz. El switch con el menor valor tiene la más alta prioirdad y se selecciona como la raíz. El valor por defecto es 32768.
Edad máxima	Define el número de segundos que un switch espera sin recibir los mensajes de configuración STP antes que intente la reconfiguración. El valor por defecto para IEEE es 20 segundos; el valor para IBM es de 10 segundos.
Tiempo de saludo	Define el número de segundos entre los mensajes de configuración STP. Para IEEE e IBM, indique un número de 1 a 10. El valor por defecto es de 2 segundos.
Retraso de reenvío	Define el número de segundos que un puerto espera antes de pasar de su estado de escucha y aprendizaje STP al estado de envío. Este retraso asegura que no se forme ningún loop antes que el switch envíe un paquete. El valor por defecto para IEEE es 15 segundos; el valor para IBM es de 4 segundos.
Costo de ruta de raíz	Una medida relativa usada para determinar la ruta más favorable hacia un destino. Consulte la **Tabla Costo de ruta, página 178** para ver mayores detalles.
Puerto de raíz	El puerto al que se aplica esta configuración.
Puente de raíz	Si el switch realmente es la raíz de STP para esa VLAN, el campo indica **Sí**. De lo contrario, el campo muestra **No**, y el puerto de raíz del dispositivo aparece indicado en la columna Puerto de raíz. **NOTA** Cada switch en una instancia de spanning-tree adopta los parámetros de saludo, retraso, y edad máxima del puente de raíz, sin importar la forma en que se configure.

Tabla Costo de ruta

Esta tabla explica la configuración por defecto de costos de ruta para diferentes velocidades.

Costo de ruta	Velocidad
100	10 Mbps
19	100 Mbps
14	155 Mbps
4	1 Gbps
2	10 Gbps
1	Velocidades superiores a 10 Gbps

Snooping IGMP (switches CE520)

Para activar y desactivar Snooping IGMP y realizar las tareas de configuración relacionadas en los switches CE520, seleccione **Configurar** > **Conmutación** > **Snooping IGMP** en la barra de funciones.

Visión general

Los switches pueden reducir el flooding innecesario de los paquetes de multidifusión IP limitando la transmisión de estos paquetes a grupos de clientes que los solicitan. Cuando los clientes (estaciones finales) automáticamente se unen y abandonan grupos que reciben tráfico de multidifusión IP, los switches pueden cambiar dinámicamente su conducta de envío para unir y abandonar solicitudes. Internet Group Management Protocol (IGMP) snooping da a los switches este control.

Procedimientos

La ventana Snooping IGMP tiene esta configuración:

- Configuración para activar generalmente Snooping IGMP y VLAN individuales
- Grupos de multidifusión para ver los grupos de multidifusión

- Puerto del router de multidifusión para ver los puertos del router de multidifusión

Antes de realizar selecciones en la ficha Configuración, seleccione un dispositivo de la lista Nombre del host. Todas las opciones que elija en esta ficha se aplicarán al dispositivo seleccionado.

Siga los siguientes pasos para cambiar la configuración:

PASO 1 Activar Snooping IGMP está marcada por defecto. Desmarque la casilla sólo si desea desactivar snooping IGMP en todo el dispositivo.

PASO 2 La tabla muestra las VLAN a las que pertenecen los puertos del switch y la configuración para las VLAN. Por defecto, la opción Snooping IGMP está activada en las VLAN. Para cambiar cualquiera de estos valores por defecto, haga clic en **Modificar** y utilice la ventana Modificar configuración de Snooping IGMP. Consulte **Modificar Snooping IGMP, página 179**.

PASO 3 Cuando termine con la ventana Snooping IGMP, haga clic en **Aceptar**.

La información que aparece en la ficha Grupos de multidifusión y la ficha Puertos del router de multidifusión es de sólo lectura y no se puede modificar.

Modificar Snooping IGMP

Esta ventana aparece cuando selecciona una VLAN hace clic en **Modificar** en la ventana Snooping IGMP mientras visualiza la ficha Configuración. Utilice esta ventana para activar o desactivar Snooping IGMP en la VLAN seleccionada.

Siga estos pasos:

PASO 1 Seleccione **Activar** o **Desactivar** de la lista Estado.

PASO 2 Cuando se haya finalizado los cambios, haga clic en **Aceptar** para cerrar la ventana y volver a la ventana Snooping IGMP.

Direcciones MAC (switches CE520)

Los switches guardan las direcciones MAC (Control de acceso de medios) de los dispositivos conectados en una tabla de direcciones MAC. Se puede administrar las direcciones de esta tabla seleccionando **Configurar** > **Conmutación** > **Direcciones MAC** en la barra de funciones.

Visión general

Un switch reconoce las direcciones MAC de los dispositivos conectados, ID de VLAN y números de interfaz leyendo la dirección de origen de los paquetes que llegan. Después de eliminada la entrada, el switch la reconoce. Si el switch encuentra un paquete para un destino desconocido, éste difunde el paquete para todos los puertos de la VLAN.

A medida que las estaciones se agregan o eliminan desde la red, el switch actualiza la tabla, agregando nuevas entradas y eliminando aquellas que no están en uso. El dispositivo también actualiza la tabla de direcciones eliminando todas las direcciones dinámicas asociadas con un puerto en el cual ocurre un cambio en la membresía de la VLAN.

Un switch puede reconocer una dirección en más de una VLAN, y una dirección dinámica que éste reconozca en una VLAN se puede introducir como una dirección segura en otra VLAN. Una dirección que el switch reconozca en una VLAN es desconocida en otra VLAN hasta que se reconozca dicha dirección.

Procedimientos

Pare ver o actualizar la tabla de direcciones MAC, siga estos pasos.

PASO 1 En esa lista Nombre de host, seleccione el switch cuyas direcciones MAC guardadas desea visualizar.

Las columnas de la tabla tienen los siguientes significados.

Columna	Significado
Dirección MAC	La dirección MAC de un dispositivo adjunto.
ID de VLAN	La ID de VLAN que está configurada en la interfaz de envío.
Interfaz de salida	La interfaz a la cual se deberán enviar los paquetes recibidos si la dirección MAC del remitente coincide con la que aparece en la columna Dirección MAC.

PASO 2 *Opcional*. Para eliminar las direcciones y limpiar la tabla, haga clic en **Eliminar todas**.

PASO 3 Haga clic en **Aceptar** para cerrar la ventana.

Ventana Búsqueda de puertos (switches CE520)

Para acceder a la ventana Búsqueda de puertos, seleccione **Monitorear** > **Buscar** en la barra de funciones. Esta opción sólo está disponible si hay un switch CD520 de Cisco presente en el sitio del cliente.

Visión general

Puede buscar puertos o dispositivos en la red. Quizás desea saber el tipo, estado y velocidad de un puerto, pero no sabe su número o a que dispositivo está conectado. Usted puede encontrar informacián rápidamente si sabe algo sobre la descripción del texto que fue ingresada para el puerto. También puede buscar

dispositivos que están conectados a un dispositivo específico si conoce la dirección IP o la dirección MAC del dispositivo especificado. Para buscar puertos o dispositivos, seleccione e introduzca una frase de búsqueda, dirección IP o dirección MAC en la ventana Buscar.

Cuando obtiene los resultados de búsqueda del puerto, utilícelos para explorar la ventana Configuración del puerto, la cual le entrega información sobre los ajustes de configuración y del estado de ejecución. Cuando obtiene los resultados de búsqueda del dispositivo, utilícelos para explorar la vista Topología, la cual le ayuda a localizar los dispositivos conectados.

Procedimientos

Utilícela para buscar puertos que tengan una palabra o frase descriptiva asociada a ellos. También puede buscar dispositivos que estén conectados a un dispositivo específico ingresando la dirección IP o la dirección MAC del dispositivo especificado.

Siga estos pasos:

PASO 1 En el campo **Encontrar puertos con Descripción/Dirección IP/Dirección MAC**, introduzca una palabra o frase descriptiva, una dirección MAC o una dirección IP. Lo que usted ingresa se asocia con todos los dispositivos en la comunidad o grupo.

Introduzca la dirección MAC en el formato xxxx.xxxx.xxxx.xxxx o xx:xx:xx:xx:xx:xx, donde x es un caracter hexadecimal (0-9, a-f, A-F).

PASO 2 Haga clic en **Buscar**.

Si introdujo una descripción del puerto en el campo Buscar, los puertos que coinciden con la descripción aparecen en el área Resultados de búsqueda. Esta información aparece en una tabla.

Columna	Explicación
Puertos	El nombre del dispositivo y el número de puerto de los puertos que coinciden con la descripción.
Descripción	Descripción del puerto.

Si se hace clic en **Buscar** sin que haya texto en el campo de búsqueda, Configuration Assistant muestra una lista de todos los miembros de la comunidad, excluyendo los controladores de WLAN y sus puertos.

Si especificó una dirección IP o dirección MAC en el campo **Buscar**, la siguiente información aparece en una tabla:

Columna	Explicación
Host	El nombre del dispositivo cuya dirección IP o dirección MAC fueron ingresadas en el campo de búsqueda.
Dirección MAC	Dirección MAC del dispositivo.
Dirección IP	Dirección IP del dispositivo.
Descripción	Tipo de dispositivo.

PASO 3 Haga clic en **Aceptar** cuando termine en esta ventana.

EtherChannels (switches CE520)

Para ver o configurar grupos de puertos en switches CE520, seleccione **Configurar** > **Puertos** > **EtherChannels** en la barra de funciones.

Visión general

Los grupos de puertos Fast EtherChannel y Gigabit EtherChannel son conexiones lógicas de alta velocidad entre switches o entre switches y servidores. Los grupos de puertos también pueden proporcionar enlaces redundantes entre switches. El switch trata al grupo de puertos como un puerto lógico único; por lo tanto, cuando crea un grupo de puertos, el switch utiliza la configuración del primer puerto para todos los puertos agregados al grupo. Luego de creado el grupo, al cambiar los parámetros de membresía de STP o VLAN para un puerto en el grupo, automáticamente se cambian los parámetros para todos los puertos.

Un puerto en cada grupo lleva todos los paquetes de STP, difusión y multidifusión desconocidos.

La ventana EtherChannels muestra los grupos de puertos y le permite:

- Crear grupos de puertos Fast EtherChannel y Gigabit EtherChannel
- Eliminar puertos desde un grupo de puertos
- Cambiar el método de envío para un grupo

Procedimientos

Esta ventana aparece cuando se selecciona en la barra de funciones. También puede hacer clic aquí para iniciarla. Utilícela para visualizar los grupos de puertos EtherChannel y para:

- **Crear grupos de puertos**
- **Modificar grupos de puertos**
- **Eliminar grupos de puertos**

Comience seleccionando un dispositivo local de la lista Nombre del host. La información en el área Grupos de canal se aplica al dispositivo seleccionado.

El campo Equilibrio de carga se configura para Dirección IP de origen y destino por defecto. No se puede modificar este campo.

Su elección se aplica a todos los grupos de puerto que cree en el switch.

Esta tabla explica las columnas en el área Grupos de canal.

Columna	Explicación
Grupo	El número asignado al grupo del puerto.
Puertos	Los puertos que pertenecen al grupo.
Estado	Sea Inactivo o Activo. También puede observar que el grupo contiene interfaces de Layer 2.

Crear grupos de puertos

Puede crear hasta 6 grupos de puerto. Los puertos que forman un grupo deben ser del mismo tipo.

Revise **Restricciones de grupo de puertos, página 186** antes de utilizar este procedimiento.

Un grupo de puertos puede contener hasta 16 miembros si están en el modo LACP. De lo contrario, puede contener hasta 8 miembros.

Por defecto, un switch envía tráfico a un grupo de puertos en base a la dirección de origen del paquete. Si configura una dirección estática para un grupo de puertos, configure el switch para enviar paquetes desde la dirección estática a todos los puertos en el grupo para así eliminar la posibilidad de paquetes perdidos. Si configura el grupo de puertos para enviar paquetes en base a la dirección de destino, configure el switch para enviar paquetes destinados para la dirección estática a sólo un puerto en el grupo de puertos. De lo contrario, la dirección de destino recibe paquetes duplicados.

Para crear un grupo de puertos:

PASO 1 Haga clic en **Crear** y utilice la ventana Crear EtherChannel. Consulte **Crear grupos de puertos, página 187**.

Puede crear un grupo de puertos en el dispostivio local que seleccionó y, opcionalmente, en un dispositivo remoto.

Haga clic en **Aceptar** para que los cambios surjan efecto y cierre la ventana.

PASO 2 Haga clic en **OK** para cerrar la ventana EtherChannels.

Modificar grupos de puertos

Puede modificar un grupo de puertos:

- Agregando un puerto miembro
- Eliminando un puerto miembro
- Cambiando el modo LACP de un puerto miembro

Para realizar alguna de estas tareas, sigas estos pasos:

PASO 1 En el área Grupos de canal, seleccione la fila del grupo que desea modificar.

PASO 2 Haga clic en **Modificar** y utilice la ventana Modificar EtherChannel. Consulte **Crear grupos de puertos, página 187**.

Puede modificar un grupo de puertos en el dispostivio local que seleccionó y, opcionalmente, en un dispositivo remoto.

PASO 3 Haga clic en **Aceptar** para que los cambios surjan efecto y cierre la ventana.

PASO 4 Haga clic en **OK** para cerrar la ventana EtherChannels.

Eliminar grupos de puertos

Para eliminar un grupo de puertos, siga estos pasos:

PASO 1 En el área Grupos de canal, seleccione la fila del grupo que desea eliminar.

PASO 2 Haga clic en **Eliminar**.

PASO 3 Haga clic en **Aceptar** para cerrar la ventana.

Restricciones de grupo de puertos

Cualquier puerto puede pertenecer a un grupo de puertos, sin embargo estas restricciones se aplican:

- El rol Switch se debe aplicar al miembro del grupo de puertos.
- Ningún miembro del grupo de puertos se puede configurar para monitoreo de puertos.
- Ningún miembro del grupo de puertos se puede habilitar para seguridad de puertos.

- Los miembros del grupo de puertos deben pertenecer al mismo conjunto de VLAN y todas deben ser de acceso estático, todas de VLAN múltiples o todas de puertos troncales.
- Los puertos de acceso dinámico no se pueden agrupar con ningún otro puerto, ni siquiera con otros puertos de acceso dinámico.
- Un puerto de red no puede estar un grupo de puertos basado en el destino.

Crear grupos de puertos

Esta ventana aparece cuando hace clic en Crear en la ventana EtherChannels. Utilícela para asignar puertos locales a un grupo de puertos en el dispositivo seleccionado, y opcionalmente, para asignar puertos remotos a un grupo de puertos en un dispositivo remoto.

Sólo los puertos asignados al rol de puerto del switch aparecen en esta ventana.

Siga estos pasos:

PASO 1 Si está creando grupos de puertos en un dispositivo local y remoto, seleccione el dispositivo remoto de la lista Dispositivo remoto. En un costado de la ventana Puertos remotos, podrá observar los puertos remotos que están conectados a los puertos del dispositivo local.

Considere que las opciones para el dispositivo remoto son las mismas que para el dispositivo local. Cuando selecciona las opciones para el dispositivo local, haga lo mismo para el dispositivo remoto.

PASO 2 En el campo **Grupo**, especifique el número del grupo de puerto que está creando.

PASO 3 Marque la casilla En Grupo para cada puerto que quiera incluir como miembro del grupo.

PASO 4 Anule la columna Estado. Ésta muestra el estado de los puertos sólo en la ventana Modificar EtherChannel.

PASO 5 Haga clic en las celdas Modo para los puertos seleccionados y seleccione uno de estos valores:

- **LACP**. El puerto puede formar un enlace e iniciar el canal. El conjunto se forma si el otro extremo está ejecutando LACP en modo activo.
- **Activar (Sin LACP)**. El puerto no utilizar LACP. Sólo existe un EtherChannel utilizable si el grupo de puertos está conectado a otro grupo en este modo.

PASO 6 Haga clic en las celdas Prioridad para los puertos seleccionados e introduzca una prioridad LACP si no desea el valor por defecto (32768 para LACP).

El puerto con más alta prioridad envía los paquetes.

PASO 7 Haga clic en **Aceptar** para cerrar la ventana.

El nuevo grupo de puertos aparece en la ventana EtherChannels.

Modificar grupos de puertos

Esta ventana aparece cuando selecciona un grupo de puertos y hace clic en Modificar en la ventana EtherChannels.

Estas son las opciones de un grupo de puertos local y remoto que puede modificar:

- Los puertos que pertenecen a un grupo de puertos
- El modo de un puerto
- La prioridad de un puerto

La columna Estado muestra información sobre los puertos que pueden ayudarle a decidir si realizar modificaciones. Pueden mostrarse tres estados:

Estado	Significado
en grupo puertos	El puerto está trabajando en el grupo de puertos.
hot-standby	Ya están activos un máximo de 8 puertos LACP.
suspendido	El puerto no está trabajando temporalmente, quizás debido a una inconsistencia con otros puertos.
autónomo	El puerto está conectado a un puerto remoto que no está participando en un grupo de puertos.
inactivo	El puerto no está trabajando. Puede estar desconectado o administrativamente inactivo.

PASO 8 Haga clic en **Aceptar** cuando termine.

6

Conexiones de enrutamiento y redes

Esta sección cubre la configuración de enrutamiento de redes e incluye los siguientes temas:

- **Direcciones IP**
- **Conexión a Internet**
- **Servidor DHCP**
- **Enrutamiento estático**

Direcciones IP

Para administrar direcciones IP, seleccione **Configurar** > **Enrutamiento** > **Direcciones IP** en la barra de funciones. Consulte estos temas para obtener información sobre la activación y configuración de direcciones IP:

- **Visión general**
- **Modificación de VLAN por defecto**
- **Configuración de la interfaz**
- **Configuración del dispositivo**

PRECAUCIÓN No recomendamos que se configure direcciones IP en una conexión WAN remota Si se interrumpe la conexión a la WAN, fallará la operación y el sistema se volverá inutilizable.

Visión general

La ventana Direcciones IP tiene estas fichas:

- **Configuración de la interfaz**, para asignar o modificar una dirección IP y máscara de subred para una VLAN. Cuando realiza esta acción, la VLAN se convierte en una interfaz virtual con switch (SVI). Al crear una SVI no se activa el enrutamiento en el dispositivo.
- **Configuración del dispositivo**, para asociar un nombre de dominio con el dispositivo seleccionado

Modificación de VLAN por defecto

Las VLAN por defecto son parte de la configuración de fábrica para estos dispositivos:

- Para el UC500, se crean estas VLAN por defecto:
  - **VLAN 1**: VLAN de datos por defecto para el UC500.
  - **VLAN 100**: VLAN de voz por defecto para el UC500.
  - **BV175**: VLAN de datos inalámbrica para el UC500.
- Para el SR520, la VLAN de datos por defecto es **VLAN75**.
- Para el SR520-T1, las VLAN de datos por defecto son **LAN0** (FastEthernet0) y **LAN1** (FastEthernet1)

Se puede modificar la dirección IP y la máscara de subred para estas VLAN por defecto en la ficha **Configuración de interfaz** en la ventana Direcciones IP.

La configuración de VLAN de vos y datos por defecto para el UC500 puede modificarse por medio del Asistente de configuración de telefonía, la que deben ejecutarse en un sistema que tenga los valores por defecto de fábrica o por medio del Administrador de múltiples sitios.

PRECAUCIÓN La modificación de la dirección IP de las VLAN de datos y voz por defecto después de la configuración inicial del sistema ocasiona cambios en otras configuraciones del sistema. Cuando se cambie esta configuración, verifique que el sistema funciona como se espera.

No modifique esta configuración en una conexión WAN remota.

Si se edita el campo Red para la VLAN100 o la interfaz de VLAN1 en la ficha Conjuntos DHCP en la ventana Servidor DHCP (**Configurar** > **Enrutamiento** > **Servidor DHCP**), se obtendrá el mismo efecto que si se cambia la dirección IP de la VLAN de datos y/o voz en el dispositivo.

IMPORTANTE:

- Después de cambiar la dirección IP de la VLAN de datos por defecto, se debe ajustar manualmente toda norma de mapeo de puertos NAT personalizados definido en **Configurar** > **Seguridad** > **NAT**.
- Luego de cambiar la dirección IP de la VLAN de datos por defecto en el UC500, se debe reiniciar cualquier switch de la serie ESW500 en el sitio del cliente para renovar la versión de DHCP en el ESW500. Esta versión también podría aplicar a otros dispositivos del sitio.

La siguiente tabla describe la configuración que CCA actualiza automáticamete cuando se indica la dirección IP de cada una de estas VLAN por defecto para estos dispositivos.

Dispositivo	VLAN por defecto	Configuración que se actualiza cuando se modifica esta VLAN.
UC500	VLAN de datos (VLAN1)	La dirección IP de la VLAN de datos (VLAN1 / BV11) se configura con el nuevo valor. El intervalo existente de exclusión de direcciones DHCP se limina y se agrega uno nuevo, basado en la nueva IP de la VLAN de datos. El conjunto existente de direcciones IP se limina y se agrega uno nuevo, basado en la nueva dirección IP de la VLAN de datos. Los pares de discado que usan objetivos de sesión para apuntar hacia la ruta para la dirección IP de la VLAN de datos existente se modifican para que apunten hacia la nueva. por ejemplo, si la nueva IP de la VLAN de datos es 192.168.20.1, el par de discado usa: objetivo de sesión ipv4:192.168.20.1. Todas las ACL (listas de control de acceso) se modifican para que usen la nueva dirección IP de la VLAN de datos. Si el UC500 está detrás de un SR500: ▪ Todas las ACL que se refieren a la subred existente se modifican para que se refieran a la nueva. ▪ Las rutas estáticas desde el SR500 hasta el UC500 que se refieren a la dirección IP de la VLAN de datos existente se modifican para que usen la nueva dirección IP de la VLAN de datos. Si el UC500 está detrás de un dispositivo de seguridad SA500 y el SA500 tiene rutas estáticas hacia la VLAN de datos existente en el UC500, éstas se modifican para que apunten hacia la nueva VLAN de datos.
UC500	VLAN de voz (VLAN100)	La VLAN de datos inalámbrica del UC500 se modifica (VLAN75/BVI75) para que use el nuevo valor. Se modifica la configuración de la aplicación de control de SCCP par que se refiera a la nueva dirección IP de la VLAN de voz. Las ACL del UC500 que se refieren a la dirección IP existente de la VLAN de voz se modifican para que se refieran a la nueva. Si el UC500 está detrás de un SR500 ó SA500, las ACL en el SR500 ó SA500 que se refieren a la dirección IP de la VLAN de voz existente se modifican para referirse a la nueva dirección IP.

Dispositivo	VLAN por defecto	Configuración que se actualiza cuando se modifica esta VLAN.
SR500 y SR520-T1	VLAN de datos VLAN75 para el SR500 FastEthernet0/0, FastEthernet0/1 para el SR520-T1)	La dirección IP de la VLAN de datos (VLAN75) se configura con el nuevo valor. El intervalo existente de exclusión de direcciones DHCP se limina y se agrega uno nuevo, basado en la nueva IP de la VLAN de datos. El conjunto existente de direcciones IP se limina y se agrega uno nuevo, basado en la nueva dirección IP de la VLAN de datos. Todas las ACL (listas de control de acceso) se modifican para que usen la nueva dirección IP de la VLAN de datos. Si el UC500 está detrás del SR500: ▪ Todas las ACL que se refieren a la dirección IP de la VLAN de datos existente se modifican para que se refieran a la nueva subred ▪ Las rutas estáticas en el UC500 que se refieren a la dirección IP de la VLAN de datos del SR500 se modifican para que usen la nueva dirección IP de la VLAN de datos. Se modifican las normas de Traducción de direcciones de redes (NAT) en el SR500 para reenviar el tráfico en los puertos 5060 (SIP) y 1720 (H323) para que usen la nueva dirección IP de la LAN de datos. Las rutas por defecto para el UC500, si está conectado a un SR500 y conectadas a un sitio de clientes, también se ajustan para reflejar el nuevo valor.

Configuración de la interfaz

Comience al seleccionar un dispositivo de la lista Nombre del host.

En la columna **Nombre de interfaz**, verá los nombres de las VLAN que están configuradas en el dispositivo seleccionado. Éstas pueden ser VLAN por defecto que sean parte de la configuración por defecto de fábrica para un dispositivo o VLAN que se agregó.

- Para asignar la nueva dirección IP, haga clic en la columna Dirección IP para el dispositivo seleccionado y especifique la nueva dirección IP.
- Para asignar una nueva máscara de subred, haga clic en la cloumna Máscara de subred para el dispositivo seleccionado y especifique un nuevo valor.

Haga clic en **Aceptar** o en **Aplicar** cuando haya finalizado.

Si está conectado a la VLAN de datos por defecto en el UC500 ó SR500, se perderá la conexión al UC500 cuando se modifica la dirección IP de la VLAN de datos para la VLAN de datos del UC500 ó SR500. Cierre CCA y vuelva a iniciarlo y conéctese al dispositivo o sitio con la nueva dirección IP.

Configuración del dispositivo

PASO 1 Comience al seleccionar un dispositivo de la lista Nombre del host.

PASO 2 En el campo **Nombre de dominio**, introduzca un nombre que identifique una región de administración en la red IP. Puede que necesite preguntarle a su administrador de red para obtener esta información. Cuando el tráfico de la red no contiene un nombre de dominio, el nombre que usted introduce se añade al nombre del dispositivo y el nombre completamente calificado se agrega a la tabla de nombre de host del dispositivo.

PASO 3 Marque **Activar búsqueda de dominios** para activar los servidores para traducir los nombres de dispositivos en direcciones IP.

PASO 4 En el campo **Nuevo servidor**, introduzca el nombre de un dispositivo que desea utilizar como servidor de nombre de dominio (DNS) y luego haga clic en **Agregar**. El dispositivo se agrega a la lista Servidores actuales.

PASO 5 Para dejar de utilizar un dispositivo como servidor DNS, selecciónelo en la lista **Servidores actuales** y haga clic en **Quitar**.

PASO 6 Haga clic en **Aceptar** o **Aplicar**.

Conexión a Internet

Aparece la ventana Conexión a Internet cuando se seleccione **Configurar** > **Enrutamiento** > **Conexión a Internet** en la barra de funciones.

Visión general

La ventana Conexión a Internet tiene dos fichas:

- **Configuración de conexión**: Para activar y configurar la conexión WAN a Internet y configurar los valores DDNS (Servicio de nombre de dominio dinámico).

- **Morfología de tráfico**: Para activar la morfología de tráfico y configurar Calidad de servicio (QoS) (recomendado para implementaciones de múltiples sitios).

Configuración de conexión

En esta ficha, se activa y configura la conexión a Internet. Se admiten los siguientes tipos de conexiones:

- **PPPoE** o **PPPoE con una dirección IP negociada**: Múltiples hosts pueden utilizar PPPoE en una interfaz Ethernet compartida para abrir sesiones de PPP a múltiples destinos con uno o más módems de puenteo. Si se selecciona una direccion IP, el router obtiene una dirección IP por medio de una negociación PPP/IPCP (Protocolo Punto a Punto/Protocolo de Control IP).
- **Dirección IP estática**: Configure la interfaz que usará una dirección IP estática:
- **DHCP**: Configure la interfaz para obtener una dirección IP desde un servidor DHCP.

También se puede realizar la configuración opcional para DDNS dinámico.

Para activar y configurar una conexión a Internet, siga estos pasos:

PASO 1 Seleccione un dispositivo para configurar de la lista Nombre de host.

PASO 2 Seleccione una interfaz de la lista Interfaces de WAN.

PASO 3 Haga clic en **Modificar** para abrir la ventana Modificar conexión a Internet. Consulte **Modificar conexión a Internet, página 199**.

PASO 4 Para guardar sus cambios y cerrar la ventana, haga clic en **Aceptar**.

Morfología de tráfico

En esta ficha, se activa la Morfología de tráfico y configura QoS.

Esta configuración se utiliza principalmente en conjunto con la configuración del máximo número de llamadas simultáneas para implementaciones de múltiples sitios.

- Consulte **Configuración de Calidad de servicio (QoS), página 510** para obtener mayor información y pautas para configurar QoS para las implementaciones de múltiples sitios.

- Consulte **Máximo de llamadas (Control de admisión de llamadas), página 518** para obtener mayor información acerca de la configuración del control de admisión de llamadas basada en estos valores.

Determine la configuración según se describe en la siguiente tabla. Haga clic en **Aceptar** o **Aplicar** cuando haya finalizado.

Configuración	Descripción
Morfología de tráfico	Marque esta configuración para activar QoS y la morfología de tráfico.
Ancho de banda de subida [kbps]	Cuando está activada la **Morfología de tráfico**, especifique el ancho de banda real de subida para el sitio, según se determine con una prueba de velocidad de conexión, en kbps, o con la Velocidad de información comprometida (CIR) en el Acuerdo de nivel de servicio (SLA) para el proveedor de servicio de Internet. Los valores válidos son del 384 al 100000 kbps. Por ejemplo, si el ancho de banda de subida es de 1,8 Mbps, especifique 1800 para el ancho de banda de subida. Si no están disponibles los resultados de una prueba de velocidad ni la CIR, especifique un valor en kbps que sea el 80% del ancho de banda de subida publicitado por el ISP (Proveedor de servicio de Internet).
Reserva de medios (%)	Utilice la barra deslizante para especificar la proporción de ancho de banda de WAN que se garantizará para el tráfico de voz si está presente en la red. Lo valores válidos varían entre 1 y 95 por ciento (el 5 por ciento restante cubre las señalizaciones y otros aspectos). Por defecto es 50%. Si no hay tráfico de voz presente en el sistema, todo el ancho de banda disponible puede utilizarse para tráfico de datos.

Para obtener más información, consulte **Modificar conexión a Internet, página 199**.

Modificar conexión a Internet

Esta ventana aparece cuando hace clic en **Modificar** en la ventana Conexión a Internet.

Para activar y configurar una conexión a Internet en una interfaz o configurar DNS dinámico opcional, complete la configuración en esta ventana según se describe a continuación y haga clic en **Aceptar**.

Configuración	Descripción
Activar interfaz WAN	Cuando está marcada, esto activa una conexión a Internet.
PPPoE	Marque la casilla PPPoE para seleccionar PPPoE para la conexión a Internet, si lo exige su proveedor de servicios. Si se marca PPPoE, realice esta configuración adicional. Se obtiene de su proveedor de servicios. ▪ **Nombre de usuario**—Nombre de usuario requerido para la conexión PPPoE. ▪ **Contraseña**—Contraseña de autentificación PAP/CHAP requerida para la conexión PPPoE. ▪ **Repetir contraseña**—Repita la contraseña para confirmarla.
IP negociado	Esta opción sólo está diposnible con encapsulamientos PPPoE. Active la opción **IP negociado** si su proveedor de servicio lo exige. Cuando se actica **IP negocado**, el router obtiene una dirección IP utilizando la negociación de direcciones PPP/IPCP.

Configuración	Descripción
IP estática	Haga clic en **IP estática** para utilizar una dirección IP estática obtenida de su proveedor de servicio. Si seleccionar **IP estática**, también se debe especificar esta configuración. Se obtiene de su proveedor de servicios. ▪ **Dirección IP de Internet** ▪ **Máscara de subred** ▪ **Gateway por defecto**—Dirección IP del gateway por defecto. ▪ **Dirección IP del servidor DNS principal** (requerido) ▪ **Dirección IP del servidor DNS secundario** (opcional) Posteriormente, si se desea modificar la conexión a Internet para usar DHCP en vez de una dirección IP estática, se le solicitará quje elimine las configuraciones existentes de VPN sobre SSL y del servidor de VPN antes de continuar.
DHCP	Seleccione DHCP para que el router pida prestada una dirección IP de un servidor DHCP remoto.

Configuración	Descripción
DDNS de HTTP	
	Opcional. Realice la configuración para el Servicio de nombre de dominio dinámico (DDNS). El sitio que utilice DHCP para obtener dinámicamente una dirección IP puede utiliar el servicio de hosting DNS dinámico (DDNS) para permitir la relación entre direcciones IP dinámicas DHCP con nombres de host estáticos. También puede configurarse DDNS para servicio con una dirección IP de WAN con IP negociado. Los sitios que utilizan DHCP que también son parte de una implementación de múltiples sitios deben configurar DDNS de HTTP.
Proveedor	Seleccione un proveedor de DDNS del menú desplegable. Se debe crear su propia cuenta DDNA con uno de estos proveedores fuera de Configuration Assistant. Están disponibles estos servicios de hosting DDNS. ▪ cgi.tzo.com ▪ dup.hn.org ▪ members.dyndns.org ▪ members.easydns.com ▪ www.dynx.cx ▪ www.justlinux.com ▪ www.zoneedit.com

Configuración	Descripción
Su nombre de host	Nombre de host único para este sitio, obtenido de su proveedor de DDNS. Por lo general, un nombre de dominio completamente calificado (FQDN), por ejemplo, mihost.midominio.net, puede ser diferente para algunos servicios de DDNS. Debe registrarse el nombre de host. Configuration Assistant no valida este campo. Asegúrese que se haya especificado el nombre de host exactamente como lo especifica su proveedor de DDNS. Si está configurando una implementación de múltiples sitios, cada sitio debe tener un nombre de host DDNS único.
Nombre de usuario	Nombre de usuario de la cuenta, obtenido de su proveedor de DDNS.
Contraseña	Contraseña de la cuenta, obtenida de su proveedor de DDNS.
Confirmar contraseña	Especifique de nuevo la contraseña para confirmarla.

Para obtener más información, consulte estos temas:

- **Configuración de DDNS, página 509**
- **Configuración de Calidad de servicio (QoS), página 510**
- **Funciones de voz admitidas en múltiples sitios, página 517**

Servidor DHCP

Para configurar la configuración del servidor DHCP, seleccione **Configurar** > **Enrutamiento** > **Servidor DHCP** en la barra de funciones.

Visión general

Un conjunto de direcciones IP DHCP (Protocolo de Configuración de Host Dinámico) es un intervalo de direcciones IP que un servidor DHCP puede asignar dinámicamente a dispositivos clientes. Debido a que no todos los clientes están conectados todo el tiempo, la entrega de direcciones IP a medida que éstas se necesitan reduce la cantidad de direcciones IP necesarias para atender a un grupo de clientes al reutilizar la misma dirección IP para diferentes clientes en momentos distintos.

Para gestionar el conjunto de direcciones IP de DHCP, usted puede:

- Crear un conjunto de direcciones IP de DHCP que identifique el intervalo de direcciones IP del conjunto.
- Asociar una dirección IP específica en el conjunto a una dirección MAC específica, creando una dirección IP estática para ese dispositivo cliente. (Algunos clientes necesitan que las direcciones IP estáticas mantengan la conectividad para admitir aplicaciones en ejecución).
- Excluya la dirección IP específica del conjunto para que no el servidor DHCP no la asigne a un cliente. (Unas pocas direcciones IP del intervalo podrían hber sido asignadas por otros procesos. Para evitar conflictos, se puede excluira dichas direcciones del conjunto.)

El rango del intervalo se calcula a partir del número de la red y de la máscara de subred. Todas las direcciones IP disponibles en el nivel de nodo se incluyen en el conjunto y quedan disponibles para el servidor, a menos que estén específicamente asociadas a una dirección MAC o sean excluidas del conjunto por una excepción; el servidor ignora las direcciones asociadas y las excepciones manuales.

La ventana Servidor DHCP tiene estas fichas:

- **Conjuntos DHCP**: Mostrar, crear, modificar o eliminar un conjunto DHCP de direcciones IP.
- **Asociaciones DHCP**: Asignar manualmente direcciones IP en el conjunto DHCP a las direcciones MAC de los clientes.
- **Exclusiones DHCP**: Especificar las direcciones IP que el servidor DHCP no debe asignar (excluir) a los clientes.

Conjuntos DHCP

Un conjunto de direcciones IP DHCP (Protocolo de Configuración de Host Dinámico) es un intervalo de direcciones IP que un servidor DHCP puede asignar dinámicamente a dispositivos clientes.

Se crean dos conjuntos DHCP por defecto para el UC500: **teléfono** y **por defecto**. Estos conjuntos DHCP por defecto pueden modificarse, pero los nombres de estos conjuntos se reservan y no pueden modificarse.

- El conjunto de **teléfonos** se asocia con la VLAN de voz (VLAN 100) en el UC500. Las direcciones IP del conjunto DHCP de teléfonos se asignan a los teléfonos IP durante el auto-registro.

- El conjunto de **datos** se asocia con la VLAN de datos (VLAN 1) en el UC500. Las direcciones IP de este conjunto se asignan a dispositivos de la VLAN de datos que solicitan en una dirección IP desde el servidor DHCP.

Para mostrar las propiedades configuradas para un conjunto DHCP, haga clic en el nombre del conjunto DHCP.

Para crear un nuevo conjunto DHCP, haga clic en **Crear** y utilice la ventana Crear Conjunto DHCP. Consulte **Crear Conjunto DHCP, página 206**.

Para modificar un conjunto DHCP existente, seleccione el conjunto DHCP, haga clic en **Modificar** y utilice la ventana Modificar conjunto DHCP. Consulte **Modificar Conjunto DHCP, página 207**.

Para eliminiar un conjunto DHCP, seleccione el nombre del conjunto DHCP y haga clic en **Eliminar**. Aparecerá una ventana, advirtiéndole que si continúa, eliminará el conjunto DHCP.

Para cerrar la ventana, haga clic en **Aceptar**.

Asociaciones DHCP

Una vez que se crea un conjunto DHCP, se puede asignar manualmente las direcciones IP desde ese conjunto a los dispositivos específicos basados en su dirección MAC.

Para crear una nueva asociación DHCP, haga clic en **Crear** y utilice la ventana Crear Asociaciones DHCP. Consulte **Crear Asociaciones DHCP, página 207**.

Para modificar una asociación DHCP existente, seleccione el nombre del conjunto, haga clic en **Modificar** y utilice la ventana Modificar asociaciones DHCP. Consulte **Modificar Asociación DHCP, página 208**.

Para eliminiar una asociación DHCP, seleccione el nombre de la asociación y haga clic en **Eliminar**. Aparecerá una ventana, advirtiéndole que si continúa, eliminará la asociación DHCP.

Para cerrar la ventana, haga clic en **Aceptar**.

Exclusiones DHCP

En esta ficha, se especifican las direcciones IP individuales o intervalos de direcciones IP que se excluyen del conjunto de direcciones DHCP. Estas direcciones no pueden asignarse a los clientes DHCP.

Para crear una nueva exclusión de DHCP, haga clic en **Crear** y utilice la ventana Crear exclusión de DHCP. Consulte **Crear Exclusión DHCP, página 205**.

Para eliminar una exclusión DHCP, seleccione la direcciñon IP y haga clic en **Eliminar**.

Por defecto, estas direcciones IP se excluyen de los conjuntos DHCP:

- 10.1.1.1 hasta 10.1.1.10 (reservadas para IOS y CUE de Cisco)
- 192.168.10.1 hasta 192.168.10.10 (reservadas para el UC500)
- 10.1.1.255 y 192.168.10.255 (direcciones de difusión)

Asociaciones de conjuntos DHCP

Pueden usarse dos tipos de asociaciones de conjuntos DHCP:

- **Vinculación automática**. El servidor DHCP creará el enlace. Después que expire el tiempo de validez, el dispositivo puede obtener una nueva dirección IP.
- **Manual de enlace**. Utilice un manual vinculante si desea que este dispositivo para utilizar esta dirección IP. La validez no expira.

Crear Exclusión DHCP

Esta ventana aparece cuando se hace clic en **Crear** en la ficha Exclusión IP de DHCP de la ventana servidor DHCP.

Use este diálogo para agregar un intervalo de exclusiones de direcciones IP de DHCP.

Siga estos pasos:

PASO 1 En el campo **Dirección IP inicial**, especifique la primera dirección IP de DHCP en el intervalo que el servidor DHCP no debe asignar a clientes DHCP.

PASO 2 En el campo **Dirección IP final**, especifique la última dirección IP de DHCP en el intervalo que el servidor DHCP no debe asignar a clientes DHCP.

PASO 3 Haga clic en **Aceptar**.

Crear Conjunto DHCP

Esta ventana aparece cuando hace clic en **Crear** en la ficha Conjunto DHCP en la ventana Servidor DHCP.

Utilice este diálogo para crear un conjunto DHCP y para, opcionalmente, identificar servidores DNS, un nombre de dominio, un router por defecto, y servidores de Servicio de nombres de internet de Windows (WINS).

Para crear un conjunto DHCP, realice la configuración como se describe a continuación y haga clic en **Aceptar**.

Configuración	Descripción
Nombre	Especifique el nombre del conjunto DHCP. En el UC500, los nombres del conunto DHCP de datos y de teléfono se reservan para las VLAN de voz (VLAN100) y de datos (VLAN1).
Red	Dirección IP inicial del conjunto DHCP. Si se edita la configuración de red para los conjuntos DHCP de datos y teléfono en el UC500, se tiene el mismo efecto que si se cambia la dirección IP para estas VLAN por defecto. Consulte **Modificación de VLAN por defecto, página 192**.
Máscara de subred	Especifique la máscara de red de la subred.
Servidor DNS 1	En el campo **Servidor DNS 1**, especifique la dirección IP de un servidor DNS. Los clientes DHCP consultan a los servidores DNS para relacionar nombres de host con direcciones IP.
Servidor DNS 2	*Opcional*. En el campo **Servidor DNS 2**, especifique la dirección IP de un segundo servidor DNS.
Nombre de dominio	Especifique el nombre de un dominio. El nombre de dominio de un cliente DHCP ubica al cliente en el dominio.

Configuración	Descripción
Servidor WINS 1, Servidor 2 WINS	*Opcional*. En los campos **Servidor WINS 1** y **Servidor WINS 2**, especifique la dirección IP de los servidores WINS. Estos campos especifican los servidores WINS que están disponibles para un cliente DHCP de Microsoft.
Router por defecto	*Opcional*. En el campo **Router por Defecto** , especifique la dirección IP de un gateway por defecto. Cuando se inicia un cliente DHCP, éste comienza a enviar paquetes a su gateway por defecto. La dirección IP del gateway por defecto debe estar en la misma subred que el cliente.

Modificar Conjunto DHCP

Esta ventana aparece cuando se hace clic en **Modificar** en la ficha Conjuntos DHCP de la ventana servidor DHCP.

Utilice este diálogo para modificar un conjunto DHCP existente, incluyendo los servidores DNS, un nombre de dominio, un router por defecto, o los servidores WINS.

No se puede modificar el nombre de los conjuntos DHCP de datos y teléfonos por defecto. Toda otra configuración puede modificarse para estos conjuntos.

Consulte **Crear Conjunto DHCP, página 206** para ver una explicación de los campos de esta ventana.

Haga clic en **Aceptar** cuando termine en esta ventana.

Crear Asociaciones DHCP

Esta ventana aparece cuando se hace clic en **Crear** en la ficha Asociaciones DHCP de la ventana servidor DHCP.

Para crear una asociación DHCP, realice la configuración como se describe a continuación y haga clic en **Aceptar**.

Configuración	Descripción
Nombre	Especifique un nombre para el conjunto de direcciones del servidor DHCP

Configuración	Descripción
Dirección IP del host	Especifique la dirección IP del host.
Máscara de red	Especifique la máscara de red de la subred del host.
Dirección MAC	Especifique la dirección MAC. Especifica una dirección de hardware para el cliente o la diferente identificaciódn del cliente en forma hexadecimal separadas por puntos. Por ejemplo, 01b7.0813.8811.66.
Nombre de cliente	Especifique el nombre del cliente con carácteres ASCII estándares. El nombre del cliente no debe ser el nombre del dominio. Por ejemplo, *no* especifique el nombre mars como mars.cisco.com.

Modificar Asociación DHCP

Esta ventana aparece cuando se hace clic en **Modificar** en la ficha Asociaciones DHCP de la ventana servidor DHCP.

Utilice este diálogo para modificar una asociación DHCP.

Consulte **Crear Asociaciones DHCP, página 207** para ver una explicación de los campos de esta ventana.

Haga clic en **Aceptar** cuando termine en esta ventana.

Enrutamiento estático

Para configurar rutas estáticas, seleccione **Configurar** > **Enrutamiento** > **Enrutamiento estático** en la barra de funciones.

Utilice esta ventana para agregar una ruta estática o para eliminar una ruta estática de un router.

Visión general

Se puede agregar una ruta estática a la tabla de enrutamiento estático en un router.

- Una ruta estática está codificada por defecto en la table de enrutamiento estático del dispositivo, por lo que cualquier ruta estática que configure no se elimina de la tabla de enrutamiento hasta que sea eliminada o reemplazada.
- Una ruta estática tiene prioridad por sobre todas las rutas dinámicas y reduce el tiempo de procesamiento al determinar, rápidamente, el recorrido de un paquete. Las rutas dinámicas son aprendidas por el dispositivo, utilizando protocolos de enrutamiento IP, como RIP, necesitan un mayor tiempo de procesamiento y caducan en la tabla de enrutamiento si no se reactualizan.

En el UC500, se crea una ruta estática hacia 10.1.10.1, la interfaz de Integrated-Service-Engine-0/0, que es el módulo Cisco Unity Express (CUE). No elimine esta ruta.

Procedimientos

Comience seleccionando el dispositivo para configurar de la lista Nombre de host.

- Para agregar una ruta estática, haga clic en **Agregar** y utilice la ventana Agregar ruta estática. Consulte **Agregar ruta estática, página 209**.
- Para eliminar una ruta estática, seleccione la ruta estática que se va a eliminar, y haga clic en **Eliminar**.

Haga clic en **Aceptar** para cerrar la ventana.

Agregar ruta estática

Esta ventana aparece cuando hace clic en **Agregar** en la ventana Enrutamiento estático.

Para agregar una ruta estática a un router, configure los parámetros según se indica a continuación, luego haga clic en **Aceptar** para guardar sus cambios y cerrar la ventana.

Configuración	Descripción
Campo IP de destino/red	Especifique la dirección IP del red de destino.
Máscara de red	Especifique la máscara de subred de la red de destino.

Configuración	Descripción
IP de gateway o interfaz saliente	Seleccione una interfaz de la lista **Interfaz saliente** o seleccione **Especificar IP de gateway**. Si se seleccona **Especificar IP de gateway,** especifique la dirección IP del gateway o de la interfaz saliente en el cuadro de texto debajo de este campo.

7

Inalámbrica

Configuration Assistant entrega herramientas para la configuración de puntos de acceso y controladores LAN inalámbricos en su sistema. Esta sección cubre los siguientes temas:

- **Configuración inalámbrica segura**
- **Convertir a Punto de acceso liviano (LAP)**
- **Configuración del controlador de LAN inalámbrica**

Consulte el **Asistente de configuración inalámbrica, página 104** para obtener información sobre el uso del Asistente de configuración inalámbrica de CCA para realizar la configuración inalámbrica y sincronizar el perfil inalámbrico en los puntos de acceso y los teléfonos IP SPA525G.

Configuración inalámbrica segura

Para configurar los puntos de acceso inalámbricos, seleccione **Configurar** > **WLAN (SSID)** en la barra de funciones.

En la ventana WLAN (SSID), usted puede:

- Configurar los parámetros SSID para la seguridad inalámbrica
- Seleccionar si se activa o no la transmisión de SSID
- Ver la configuración de seguridad que se realizó en el punto de acceso
- Configurar servidores RADIUS
- Configurar parámetros de radio inalámbrica para los puntos de acceso autónomos
- Configurar la autenticación MAC para los puntos de acceso AP541N
- Activar o desactivar la interfaz inalámbrica para los dispositivos UC500 y SR500 con capacidades inalámbricas integradas.

NOTA Para desactivar la función inalámbrica para los dispositivos UC500 y SR500 con capacidad inalámbrica integrada, desmarque la opción **Activar interfaz inalámbrica** en la ventana WLAN (SSID). Por defecto, la interfaz inalámbrica se activa para estas plataformas.

La configuración inalámbrica varía, dependiendo del tipo de punto de acceso que se está configurando:

- **Configuración inalámbrica para los puntos de acceso AP541N de Cisco**
- **Configuración inalámbrica para los puntos de acceso incorporados AP521 y UC500 ó SR500 de Cisco.**

Configuración inalámbrica para los puntos de acceso AP541N de Cisco

Las siguientes secciones explican la configuiración inalámbrica en cada una de las fichas de la ventana WLAN (SSID) para los puntos de acceso de radio única y doble banda AP541N de Cisco.

- **SSID**
- **Radius**
- **Autenticación MAC**

NOTA Para configurar funciones en el AP541N que no se administren actualmente por medio de CCA, tal como agrupación, use la Utilidad de configuración de AP541N. Para acceder a esta utilidad, haga clic con el botón derecho en el icono de AP541N en la vista Topología y seleccione la Utilidad de configuración en el menú emergente.

SSID

En la ficha SSID, se puede ver, crear o modificar los SSID y sus configuraciones asociadas para los puntos de acceso AP541N

Pueden crearse hasta diesicéis (16) SSID en un soplo punto de acceso AP541N.

- Para crear nuevos SSID, haga clic en **Crear** para abrir la ventana Crear o Modificar SSID.
- Para modificar la configuración de un SSID existente, seleccione el SSID de la lista y haga clic en **Modificar**.

Para ver información detallada sobre la configuración de SSID para los puntos de acceso AP541N, consulte **Crear o Modificar SSID para los puntos de acceso AP541N de Cisco, página 223**.

Esta tabla explica la configuración que se muestra en la ventana de SSID.

Configuración	Descripción
SSID	El Identificador de conjunto de servicios configurado en el punto de acceso. El nombre de SSID no puede modificarse una vez creado. Para cambiar su nombre, elimina el SSID y cree uno nuevo con un nombre diferente. Los SSID de cisco-data (VLAN1) y cisco-voice (VLAN100) son los SSID por defecto para el tráfico de voz y datos. Por defecto, estos SSID tiene la seguridad configurada como Ninguna. Para acceder a la configuración de seguridad de un SSID existente por defecto, seleccione el SSID y haga clic en **Modificar**.
VLAN	Muestra la VLAN asociada con el SSID.
Seguridad	Muestra el tipo de seguridad inalámbrica y su configuración asociada. Para el AP541N, se admiten los siguientes tipos de segurida: ▪ Ninguno ▪ WEP estática ▪ WEP dinámica ▪ WPA Personal ▪ WPA Empresarial Consulte **Opciones de seguridad inalámbrica para dispositivos AP541N, página 226** para ver una descripción de cada opción.
Cifrado	Muestra uno de los siguientes tipos de cifrado inalámbrico, basado en el tipo de seguridad seleccionado: Ninguna, **WEP**, **AES**, o **TKIP** y **AES CCMP**.

Configuración	Descripción
Autenticación	Muestra uno o más de los siguientes tipos de autenticación, basado en el tipo de seguridad seleccionado. ▪ Ninguno ▪ **autenticación abierta** ▪ **autenticación abierta con EAP** ▪ **EAP de red**
Tipo de autenticación MAC	Se puede configurar una lista global de direcciones MAC a las que se les permite o niega el acceso a la red. Seleccione uno de los siguientes tipos de Autenticación MAC: ▪ **Local**—Usa la lista de Autenticación MAC que se configura en la ficha Autenticación MAC. Consulte **Autenticación MAC, página 216**. ▪ **Radius**—Usa la lista de Autenticación MAC que se configura en el servidor RADIUS externo. ▪ **Desactivada**—No usa la Autenticación MAC.

Radius

En la ficha Radius, se puede activar y configurar los parámetros globales para los servidores RADIUS externos para la contabilidad y autenticación de los clientes inalámbricos. El AP541N no tiene un servidor RADIUS local.

Configuración	Descripción
Dirección IP de RADIUS	Especifique la dirección para el servidor RADIUS global primario. Cuando el primer cliente inalámbrico trate de autenticarse en el AP, éste envía una solicitud de autenticación al servidor primario. Si éste servidor responde a la solicitud de autenticación, el AP sigue usando este servidor RADIUS como el servidor primario, y las solicitudes de autenticación se envían a la dirección que se especifique.

Configuración	Descripción
Dirección IP 1 de RADIUS, Dirección IP 2 de RADIUS, Dirección IP 3 de RADIUS	Especifique hasta tres direcciones IPv4 para los servidores RADIUS de copia de respaldo. Si falla la autenticación con el servidor primario, se le pregunta a cada servidor configurado en secuencia. La dirección dbe ser válida para que el AP intente comunicarse con el servidor.
Clave RADIUS	La clave RADIUS es la clave secreta compartida para el servidor RADIUS global primario. Se puede especificar hasta 63 caracteres alfanuméricos y especiales para la clave RADIUS. La clave es sensible a las mayúsculas y debe configurar la misma clave en el AP y en su servidor RADIUS. La clave RADIUS no se muestra en texto plano mientras se escribe.
Clave RADIUS 1, Clave RADIUS 2, Clave RADIUS 3	Especifique la clave RADIUS asociada a cada uno de los servidores RADIUS de copia de respaldo configurados. El servidor en la Dirección IP RADIUS 1 usa la clave RADIUS 1, el servidor en la Dirección IP RADIUS 2 usa la clave RADIUS 2, y así sucesivamente. Se puede especificar hasta 63 caracteres alfanuméricos y especiales para la clave RADIUS. La clave es sensible a las mayúsculas y debe configurar la misma clave en el AP y en su servidor RADIUS. La clave RADIUS no se muestra en texto plano mientras se escribe.
Activar Cuenta de RADIUS	Active esta opción para dar seguimiento y medir los recursos que un usuario específico ha consumido, como tiempo del sistema, cantidad de datos recibidos y transmitidos, etc. Si se activa la cuenta de RADIUS, se activa para el servidor RADIUS primario y para todos los servidores de copia de respaldo.

Autenticación MAC

En la ficha Autenticación MAC, se especifica una lista de direcciones MAC para controlar el acceso a la red por medio del AP basado en la dirección MAC del cliente inalámbrico. También se especifica si a los clientes con aquellas direcciones MAC se les permite o niega el acceso a la red. Esta lista local se usa cuando **Autenticación MAC** se configura como Local para un SSID configurado en el AP541N.

Para configurar la autenticación MAC, siga estos pasos:

PASO 1 Seleccione cómo desea filtrar los clientes con las direcciones MAC especificadas en la lista.

- Seleccione **Permitir direcciones de la lista** para sólo permitir el acceso a los clientes con las direcciones MAC especificadas en la lista.
- Seleccione **Denegar direcciones de la lista** para permitir el acceso a todos los clientes, excepto aquellos con las direcciones MAC especificadas en la lista.

PASO 2 Haga clic en **Agregar** para crear una nueva fila en la tabla.

PASO 3 Haga clic en cualquier parte de la fila y especifique la dirección MAC hexadecimal d 12 dígitos para el cliente que se va a agregar a la lista.

Especifique las direcciones MAC usando el formato `xxxx.xxxx.xxxx` (por ejemplo, `0101.FEFE.2345`). Los caracteres punto (.) se agregan automáticamente mientras se escribe. No use dos puntos (:) para separar los dígitos hexadecimales en la dirección MAC.

PASO 4 Siga agregando direcciones MAC a la lista, según sea necesario.

PASO 5 Haga clic en **Aceptar** o en **Aplicar** cuando haya finalizado.

Para eliminar una dirección MAC de la lista, destaque la dirección y haga clic en **Eliminar**, luego haga clic en **Aplicar** o **Aceptar**.

Configuración inalámbrica para los puntos de acceso incorporados AP521 y UC500 ó SR500 de Cisco.

Las siguientes secciones explican la configuración de cada una de las tres fichas de la ventana WLAN (SSID):

- **Nombres de redes inalámabricas (SSID)**

- **Servidores RADIUS**
- **Configuración de puntos de acceso**

NOTA Los routers seguros SR500 con puntos de acceso incorporados tienen configuraciones similares, pero el GUI para realizar esta configuración no tiene fichas separadas. Consulte las secciones **Nombres de redes inalámabricas (SSID)** y **Servidores RADIUS** para ver información acerca de esta configuración.

Nombres de redes inalámabricas (SSID)

Se puede configurar funciones de seguridad en su **Punto de acceso autónomo**. Las funciones de seguridad protegen las comunicaciones entre el punto de acceso autónomo y otros dispositivos inalámbricos y evitar el acceso no autorizado. Se puede configurar diferentes niveles de seguridad y cifrado en sus puntos de acceso autónomos. Los niveles de seguridad varían entre nada de seguridad y alta seguridad.

Esta tabla explica las columnas de la ventana.

Configuración	Descripción
SSID	El Identificador de conjunto de servicios configurado en el punto de acceso.
VLAN	La VLAN asociada con el SSID.
Activar interfaz inalámbrica	Esta opción sólo aparece para los dispositivos UC500 y SR500 con capacidades inalámbricas integradas. Cuando no se marca esta opción, la interfaz inalámbrica de estos dispositivos se apaga. Se puede configurar SSID y parámetros cuando la interfaz inalámbrica se apaga.

Configuración	Descripción
Seguridad	Tipo de seguridad inalámbrica y configuración asociada: ▪ Nada de seguridad ▪ **WEP, página 230** ▪ **EAP, página 231** ▪ **LEAP, página 231** ▪ **WPA, página 232** ▪ **WPA-PSK, página 232** ▪ **WPA2, página 233** ▪ **WPA2-PSK, página 233** ▪ **MAC, página 233** ▪ **MAC y EAP, página 234** ▪ Desconocido. Esto parece si la configuración de seguridad se configura mediante la interfaz de línea de comandos y la configuración de seguridad no es compatible con el Asistente de configuración.
Cifrado	Tipo de cifrado inalámbrico: ▪ Ninguno (no se recomienda) ▪ **WEP** ▪ Dinámica **WEP** ▪ **TKIP** ▪ **AES CCMP**
Autenticación	Uno o más de estos tipos de autenticación: ▪ **autenticación abierta** ▪ **autenticación abierta con EAP** ▪ **EAP de red** ▪ **WPA-PSK**

Siga estos pasos para configurar los SSID y activar la seguridad para sus puntos de acceso autónomos.

PASO 1 En la lista **Nombre de host**, seleccione un punto de acceso.

PASO 2 Para crear una LAN inalámbrica y seleccionar la configuración de seguridad, seleccione los Nombres de redes inalámbricas (SSID), haga clic en la ficha **Crear**, y complete la ventana Crear WLAN. Consulte **Crear o Modificar SSID de WLAN, página 223**.

Múltiples WLAN permiten a los usuarios acceder a diferentes redes por medio de un solo punto de acceso autónomo.

El número de SSID que se puede crear varía, dependiendo del tipo de punto de acceso que se configure. Por ejemplo, los dispositivos SR500 admiten un máximo de cuatro (4) SSID.

PASO 3 Para modificar una configuración, seleccione la WLAN, haga clic en **Modificar**, y use la ventana Modificar WLAN. Consulte **Crear o Modificar SSID de WLAN, página 223**.

PASO 4 Para eliminar una configuración, seleccione la WLAN, y haga clic en **Eliminar**.

PASO 5 Para apagar la interfaz inalámbrica para UC500 y SR500, desmarque la opción **Activar interfaz inalámbrica**. Puede crear y modificar los SSID mientras la interfaz esté apagada. Por defecto, está activa la interfaz inalámbrica.

PASO 6 Para aplicar sus cambios y cerrar la ventana, haga clic en **Aceptar**.

Servidores RADIUS

En esta ficha, se puede:

- Configurar un servidor RADIUS para los clientes inalámbricos, agregar usuarios de WLAN y configurar contraseñas de usuarios o
- Activar y configurar un servidor RADIUS externo para las cuentas y autenticación de los clientes inalámbricos.

Las opciones de configuración del servidor Servicio de usuario de acceso telefónico de Autentificación Remota (RADIUS) sólo están disponibles si el UC500 tiene un punto de acceso integrado o si el sitio del cliente tiene un controlador LAN inalámbrico.

Configure al servidor RADIUS como se describe en esta tabla, luego haga clic en **Aceptar** o **Aplicar**.

Columna	Descripción
Su nombre de host	Seleccione un nombre de host de la lista desplegable.
Servidor RADIUS externo	
Activar servidor RADIUS externo	Cuando se marca esta opción, se activa la configuración de un servidor RADIUS externo para la autenticación de clientes inalámbricos.
Dirección IP	Dirección IP del servidor RADIUS externo.
Clave secreta	Clave secreta compartida que usa el controlador de WLAN o el punto de acceso para comunicarse con el servidor RADIUS externo.
Puerto de autenticación	Número del puerto de autenticación del servidor RADIUS. El valor por defecto es 1812.
Puerto de cuentas	Número del puerto de cuentas del servidor RADIUS. El valor por defecto es 1813.
Servidor RADIUS local	
Activar servidor RADIUS local	Cuando se marca esta opción, se activa la configuración de un servidor RADIUS local para la autenticación de clientes inalámbricos.
Clave secreta	Clave secreta compartida que usa el controlador de WLAN o el punto de acceso para comunicarse con el servidor RADIUS local.
Usuarios	Nombre de usuario y contraseña para cada cliente que puede autenticarse usando el servidor RADIUS local. Haga clic en **Agregar** para insertar una nueva fila en la table y especifique un nombre de usuario y contraseña.

Columna	Descripción
Direcciones MAC	Las direcciones MAC de los cliente que pueden autenticarse usando el servidor RADIUS local. Haga clic en **Agregar** para insertar una nueva fila en la tabla y especifique la dirección MAC en formato xxxx.xxxx.xxxx.xxxx. Por ejemplo: 105b.aaab.99ac.0056

Configuración de puntos de acceso

Configure al Punto de acceso como se describe en esta tabla, luego haga clic en **Aceptar** o **Aplicar**.

Parámetro	Descripción
Configuración de canal	
La selección disponible de canales de radio la determina su dominio regulador.	
Canal	Seleccione el canal de radio que se usará para este punto de acceso. Cuando se selecciona Frecuencia con menor congestión para la configuración del canal, el dispositivo busca el canal de radio que esté menos ocupado y lo selecciona para usarlo. El dispositivo busca el encenderse y cuando se cambia la configuración de radio. También se puede seleccionar la configuración del canal específico en el menú desplegable.
Configuración de modo mundial	
Activar modo mundial	
Puede configurar el dispositivo inalámbrico para que admita el modo mundial. Cuando se activa el modo mundial, el dispositivo inalámbrico agreagr información fija del portador del canal a su baliza. Los dispositovos del cliente con el modo mundial activado reciben la información fija del portador y ajustan sus parámetros automáticamente. Por ejemplo, un dispositivo cliente usado principalmente en Japón podría apoyarse en el modo mundial para ajustar su configuración de energía y de canal automáticamente cuando viaje a Italia y se conecte a una red allá.	

Parámetro	Descripción
País	Seleccione el país principal para este punto de acceso.
Ubicación	Seleccione al aire libre, bajo techo, o ambos para indicar la ubicación del punto de acceso.

Nivel de potencia

La configuración del Nivel de potencia determina el nivel de potenci de la transmisión de radio.

La configuración de potencia por defecto es la más alta potencia de transmisión permitida en su dominio regulador. Las normativas gubernamentales definen el máximo nivel de potencia permitido para los dispositivos de radio. Esta configuración debe ajustarse a los estándares establecidos para el país en que se usa el dispositivo. Para reducir la interferencia, limite el alcance de su punto de acceso; para ahorar energía, seleccione un nivel de potencia más bajo.

Para una radio de 802.11g, la configuración de Potencia de transmisión se divide en Potencia de trasmisor CCK (dBm) y Potencia del transmisor OFDM (dBm). La configuración de potencia puede estar en mW o en dBm, dependiendo de la radio en particular que se configure. La Tabla de traducción de potencia (consulte **Tabla de traducción de potencia, página 223**) traduce tanto mW como dBm.

Potencia de trasmisor CCK (dBm)	CCK es la modulación usada en 802.11g para los niveles de frecuencia más bajos. En la mayoría de los casos, se puede seleccionar Máximo; las selecciones disponibles varían entre 3dBm y 17 dBm.
Potencia de trasmisor OFDM (dBm)	OFDM es la modulación usada en 802.11g para velocidades de datos más alatas (sobre 20 Mbps). En la mayoría de los casos, se puede seleccionar Máximo; las selecciones disponibles varían entre 3 dBm y 17 dBm.
Potencia de cliente (dBm)	la Potencia de cliente determina en nivel máximo de potencia permitido en los dispositivos de clientes que se asocian al punto de acceso. Cuando un dispositivo cliente se asocia al punto de acceso, éste envía la configuración del nivel máximo de potencia al cliente. En la mayoría de los casos, se puede seleccionar Máximo; las selecciones disponibles varían entre 3dBm y 17 dBm.

Parámetro	Descripción
Configuración de antena (sólo SKU inalámbricos para UC520 y UC540)	
Sólo se deben modificar estas configuraciones de antena si Soporte de Cisco lo indica. Los SKU inalámbricos para UC520 y UC540 sólo tienen una antena.	
Antena de recepción	Para los SKU inalámbricos para UC520 y UC540, la antena receptora debe configurarse como **Primaria**.
Antena de transmisión	Para los SKU inalámbricos para UC520 y UC540, la antena transmisora debe configurarse como **Primaria**.

Tabla de traducción de potencia

Traducción aproximada entre mW y dBm																					
dBm	-1	2	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
mW	1	2	3	4	5	6	8	10	12	15	20	25	30	40	50	60	80	100	125	150	200	250

Crear o Modificar SSID de WLAN

Aparece esta ventana cuando se hace clic en **Crear** o **Modificar** en la ventana WLAN (SSID). Use la ventana para crear un nuevo SSID y para especificar la configuración de seguridad para el acceso inalámbrico.

La configuración del SSID de WLAN varía, dependiendo del tipo de punto de acceso que se está configurando:

- **Crear o Modificar SSID para los puntos de acceso AP541N de Cisco**
- **Crear o modificar las SSID para los puntos de acceso incorporados AP521 ó UC500 de Cisco.**

Crear o Modificar SSID para los puntos de acceso AP541N de Cisco

Para crear un nuevo SSID para un punto de acceso AP541N de Cisco, siga estos pasos.

PASO 1 Realice una configuración básica del SSID para el AP541N como se describe en la siguiente tabla.

Configuración	Descripción
SSID	En el campo SSID, especifique un SSID. El SSID puede contener hasta 32 caracteres alfanuméricos. Las comillas (") de carácter no está permitido.
Transmisión de SSID	Especifique si se permitirá que el AP541N transmita el identificador de conjunto de servicios (SSID). Por defecto, la transmisión de SSID está desactivada. Cuando se desactiva la Transmisión de SSID, no se muestra el nombre de red en la lista de redes disponibles en un cliente. En vez de ello, el cliente debe tener el nombre de red exacto configurado antes de poder conectarse. Basta con desactivar la Transmisión de SSID para evitar que los clientes accidentalment se conecten a su red, pero ello no evita ni los más simples intentos de un hacker de conectarse o monitorear el tráfico cifrado. La supresión de la transmisión SSID ofrece un muy bajo nivel de protección en una red de otra manera expuesta (como una red invitada) donde la prioridad es facilitar que los clientes se conecten y donde no hay información sensible disponible.
VLAN	Especifique la ID de VLAN asociada con este SSID. Los valores válidos son del 1 al 4094. La VLAN por defecto para el tráfico de voz es VLAN100 y la VLAN por defecto para el tráfico de datos es VLAN1. CCA no verifica para asegurarse que existe la VLAN en la red, así que usted debe estar seguro de especificar una ID de VLAN válida en este campo.

PASO 2 En la sección **Seguridad Configuración** de la ventana, seleccione el tipo deseguridad que se va a usar para este SSID y configure la configuración adicional requerida para ese tipo de seguridad.

La configuración varía, dependiendo del tipo de seguridad seleccionada. Para ver información detallada acerca de cada tipo de seguridad y su configuración asociada, consulte**Opciones de seguridad inalámbrica para dispositivos AP541N, página 226**.

PASO 3 Seleccione el **Tipo de autenticación MAC**.

Configuración	Descripción
Desactivado	No usa la Autenticación MAC.
Local	lse la lista de Autenticación MAC que se configuró en la ficha Autenticación MAC de la ficha Inalámbrica (SSID). Consulte **Autenticación MAC, página 216**.
Radius	Usa la lista de Autenticación MAC que se configura en el servidor RADIUS externo.

PASO 4 Haga clic en **Aceptar** o **Aplicar**.

Crear o modificar las SSID para los puntos de acceso incorporados AP521 ó UC500 de Cisco.

Para crear o modificar SSID para los puntos de acceso AP521 y UC500 incorporados, siga estos pasos:

PASO 1 En el campo **SSID**, especifique un SSID. El SSID puede contener hasta 32 caracteres alfanuméricos.

PASO 2 Marque **Transmisión en Beacon** si desea transmitir la SSID para que los dispositivos que no especifican un SSID puedan asociarse (establecer una conexión inalámbrica) con el punto de acceso autónomo. Sólo un SSID puede inlcuirse en el Beacon (la SSID invitada).

PASO 3 En el campo **VLAN**, especifique o seleccione la ID de VLAN que desea asociar con el SSID.

Si se asigna una VLAN a cualquier SSID, se debe asignar una VLAN a cada SSID. No se puede tener algunos SSID asignados a VLAN y otros asigandoa a *ninguno*.

PASO 4 Marque la casilla **VLAN Nativa** si desea que esta VLAN sea la **VLAN nativa**.

PASO 5 En el área Configuración de seguridad, seleccione la configuración de seguridad de la lista **Seguridad**. Las restantes opciones de esta ventana dependen de lo que se seleccione.

Se puede seleccionar **Nada de seguridad**, **WEP**, **EAP**, **LEAP**, **WPA**, **WPA-PSK**, **WPA2**,**WPA2-PSK**, **MAC**, o **MAC y EAP**.

Consulte **Opciones de seguridad inalámbrica para dispositivos UC500W y AP541N, página 230** para ver una descripción de cada configuración.

Configuration Assistant automáticamente selecciona el cifrado y el tipo de autenticación, dependiendo de la configuración de seguridad que se haya seleccionado.

PASO 6 Haga clic en **Aceptar** para guardar sus cambios y cerrar la ventana.

Opciones de seguridad inalámbrica para dispositivos AP541N

Esta sección describe las opciones de seguridad inalámbrica y su configuración relacionada para los puntos de acceso AP541N.

Ninguno

Si se selecciona **Ninguno** como el modo de seguridad, no se necesita configuración de seguridad adicional. Los datos transferidos hacia y desde el punto de acceso no están cifrados y no se realiza autenticación. Este modo puede ser útil durante la configuración inicial de la red o para solucionar problemas, pero no se recomienda para el uso regular en la red interna porque no es seguro.

WEP estática

La configuración de seguridad **WEP estática** necesita que el punto de acceso autónomo y el dispositivo cliente (el dispositivo que se conecta al dispositivo inalámbrico, como un laptop o una PC) compartan la misma clave WEP para mantener la comunicación privada.

WEP estática no es el modo más seguro disponible, pero ofrece más protección que si se configura el modo de seguridad como Ninguno (texto plano).

Si se selecciona **WEP estática**, configure estos parámetros adicionales.

Configuración	Descripción
Cifrado	Sólo lectura. Se usa el cifrado AES.
Autenticación	Sólo lectura. Se usa la autenticación EAP de red.

Configuración	Descripción
Longitud de la clave	Seleccione 64 bits ó 128 bits para la longitud de la clave de cifrado.
Tipo de clave	Seleccione **ASCII** o **HEX** (hexadecimal).
Clave	Se puede especificar hasta cuatro claves WEP. Para cada clave, especifique una cadena de caracteres. Use el mismo número de caracteres para cada clave. Se trata de claves WEP compartidas con las estaciones que usan el AP. Las claves que se especifiquen dependen del tipo de clave seleccionado. **ASCII**. Incluye letras en mayúscula y minúscula, dígitos numéricos y símbolos especiales como @ y #. **Hex**. Incluye dígitos 0 a 0 y las letras a hasta la F. El número de caracteres que se especifican en los campos Clave se determina según la Longitud de clave y Tipo de clave que se seleccione. Por ejemplo, si se usa claves ASCII de 128 bits, la clave WEP debe tener 13 caracteres.

WEP dinámica

WEP dinámica entrega claves generadas dinámicamente que se actualizan periódicamente.

Este modo necesita el uso de un servidor RADIUS externo para autenticar los usuarios. El AP necesita un servidor RADIUS capaz de EAP, como Internet Authentication Server de Microsoft. Para trabajar con los clientes de Windows, el servidor de autenticación debe admitir EAP protegido (PEAP) y MSCHAP V2.

Si se selecciona WEP estática para seguridad, configure estos parámetros adicionales.

Configuración	Descripción
Cifrado	Sólo lectura. Se usa el cifrado AES.
Autenticación	Sólo lectura. Se usa la autenticación EAP de red.

Configuración	Descripción
Servidor activo	Muestra el servidor RADIUS que está en uso. Se puede actualizar manualmente el servidor seleccionando un servidor diferente en la lista desplegable. **NOTA** El servidor activo no se guarda de un reinicio y otro. El primer servidor RADIUS configurado se selecciona al reiniciar.
Velocidad de actualización de claves de transmisión	Especifique un valor para fijar el intervalo al que se actualiza la clave de transmisión (grupo) para los clientes asociados a este SSID. Los valores válidos varían entre 1 y 86400 segundos. Un valor de 0 incida que la clave de transmisión no se actualiza.
Velocidad de actualización de claves de sesión	Especifique un valor para fijar el intervalo en el que AP actualizará las claves de sesión (unidifusión) para cada cliente asociado con este SSID. El intervalo válido es de 0 a 86400 segundos. Un valor de 0 incida que la clave de transmisión no se actualiza.

WPA Personal

WPA Personal es un estándar de Wi-Fi Alliance IEEE 802.11i que incluye AES-CCMP y cifrado TKIP. La versión personal de WPA emplea una clave previamente compartida (en vez de usar IEEE 802.1X) y EAP como se usa en el modo de seguridad WPA Empresarial. La clavem previamente compartida (PSK) se usa sólo para una verificación inicial de credenciales.

Este modo de seguridad es compatible en reversa para los clientes inalámbricos que admiten el WPA origial.

Si se selecciona **WEP Personal**, configure estos parámetros adicionales.

Configuración	Descripción
Cifrado	Sólo lectura. Se usa TKIP, AES-CCM P.
Autenticación	Sólo lectura. Se usa la autenticación EAP de red con EAP abierta.

Configuración	Descripción
Clave	Especifique la clave secreta previamente compartida para la seguridad WPA Personal. La clave puede contener desde 8 hasta 63 caracteres. Los caracteres aceptables incluyen letras en mayúscula y minúscula, dígitos numéricos de 0 a 9, y símbolos especiales como @ y #.
Velocidad de actualización de claves de transmisión	Especifique un valor entre 0 y 86400 segundos para fijar el intervalo al que se actualiza la clave de transmisión (grupo) para los clientes asociados. Un valor de 0 incida que la clave de transmisión no se actualiza.

WPA Empresarial

WPA Empresarial con RADIUS es una implementación del estándar Wi-Fi Alliance IEEE 802.11i, que incluye CCMP (AES), y mecanismos TKIP. El modo WPA Empresarial necesita el uso de un servidor RADIUS para autenticar usuarios.

Este modo de seguridad es compatible en reversa con los clientes inalámbricos que admiten el WPA origial.

Si se selecciona WEP estática, configure estos parámetros adicionales.

Configuración	Descripción
Cifrado	Sólo lectura. Se selecciona tanto TKIP como AES-CCMP. Cuando se selecciona tanto TKIP como CCMP, los clientes configurados para usar WPA con RADIUS deben tener uno de lo indicado a continuación: ▪ Una dirección IP TKIP RADIUS y una clave RADIUS válidas ▪ Una dirección IP CCM (AES) y una clave RADIUS válidas
Servidor activo	Muestra el servidor RADIUS que está en uso. Se puede actualizar manualmente el servidor seleccionando un servidor diferente en la lista desplegable. **NOTA** El servidor activo no se guarda de un reinicio y otro. El primer servidor RADIUS configurado se selecciona al reiniciar.

Configuración	Descripción
Velocidad de actualización de claves de transmisión	Especifique un valor para fijar el intervalo al que se actualiza la clave de transmisión (grupo) para los clientes asociados a este AP. Los valores válidos varían entre 1 y 86400 segundos. Un valor de 0 incida que la clave de transmisión no se actualiza.
Velocidad de actualización de claves de sesión	Especifique un valor para fijar el intervalo en el que AP actualizará las claves de sesión (unidifusión) para cada cliente asociado. El intervalo válido es de 0 a 86400 segundos. Un valor de 0 incida que la clave de transmisión no se actualiza.

Opciones de seguridad inalámbrica para dispositivos UC500W y AP541N

Esta sección describe las opciones de seguridad inalámbrica y parámetros relacionados para los puntos de acceso AP521 y plataformas UC500 que tienen un punto de acceso integrado.

Nada de seguridad

Esta es la opción menos segura. Selecciónela sólo para un SSID que se use en un lugar público (SSID invitada) y asóciela con una VLAN que restrinja el acceso a su red. No hay cifrado, y el tipo de autenticación es **autenticación abierta**

WEP

Esta configuración de seguridad necesita que el punto de acceso autónomo y el dispositivo cliente (el dispositivo que se conecta al dispositivo inalámbrico, como un laptop o una PC) compartan la misma clave **WEP** para mantener la comunicación privada. El tipo de cifrado es WEP, y el tipo de autenticación es **autenticación abierta**

Para configurar este tipo de seguridad:

PASO 1 Especifique una frase secreta en el campo **Frase secreta**, y seleccione el cifrado de bits de la lista.

PASO 2 Haga clic en **Generar**. El campo de claves ubicado al lado de la lista **Clave** se llena automáticamente. Puede cambiar el número de la clave seleccionando 1, 2, 3, ó 4 en la lista **Clave**. El número de la clave por defecto es 1.

EAP

Esta configuración de seguridad activa la autenticación IEEE 802.1X y necesita que se indique la dirección IP y clave secreta compartida para un servidor **RADIUS**. El tipo de cifrado es **WEP** dinámica, y el tipo de autenticación es **autenticación abierta con EAP**

Si se selecciona el tipo de seguridad EAP, los clientes inalámbricos deben usar la configuracion EAP (por ejemplo, EAP-TLS, EAP-FAST, ó PEAP). Los clientes inalámbricos no pueden usar la configuración LEAP.

Para configurar este tipo de seguridad:

PASO 1 Especifique la dirección IP del servidor RADIUS.

PASO 2 Especifique el secreto compartido que el punto de acceso autónomo usarñá para comunicarse con el servidor RADIUS.

LEAP

Esta configuración de seguridad activa la autenticación IEEE 802.1X y necesita que se indique la dirección IP y clave secreta compartida para un servidor **RADIUS**. El tipo de cifrado es WEP dinámica, y los tipos de autenticación son **autenticación abierta con EAP** y **EAP de red**.

Notas

- Si se selecciona el tipo de seguridad LEAP, los clientes inalámbricos deben usar la configuración LEAP.
- Configuration Assistant activa tanto la Autenticación abierta con EAP como la Autenticación EAP de redes para permitir que tanto los dispositivos clientes de Cisco como los que no son clientes de Cisco se asocien con el

punto de acceso autónomo usando el mismo SSID para realizar la autenticación IEEE 802.1x.

Para configurar este tipo de seguridad:

PASO 1 Especifique la dirección IP del servidor RADIUS.

PASO 2 Especifique el secreto compartido que el punto de acceso autónomo usarñá para comunicarse con el servidor RADIUS.

WPA

Esta configuración de seguridad es más segura que la configuración EAP. Activa la autenticación **WPA** y necesita que se indique la dirección IP y el secreto compartido para un servidor RADIUS. Los dispositivos clientes que se asocian al punto de acceso autónomo usando este SSID deben tener capacidad WPA. El tipo de cifrado es **TKIP**, y los tipos de autenticación son **autenticación abierta con EAP** y **EAP de red**.

Configuration Assistant activa tanto la **Autenticación abierta con EAP** como la **Autenticación EAP de redes** para permitir que tanto los dispositivos clientes de Cisco como los que no son clientes de Cisco se asocien con el punto de acceso autónomo usando el mismo SSID para realizar la autenticación IEEE 802.1x.

Para configurar este tipo de seguridad:

PASO 1 Especifique la dirección IP del servidor RADIUS.

PASO 2 Especifique el secreto compartido que el punto de acceso autónomo usarñá para comunicarse con el servidor RADIUS.

WPA-PSK

Seleccione esta configuración de seguridad cuando desee usar el cifrado WPA y no se tiene acceso a un servidor RADIUS. El punto de acceso aautónomo y el cliente deben compartir la misma **WPA-PSK**. La clave puede tener entre 8 y 63 caracteres de largo. El tipo de cifrado es **TKIP**, y el tipo de autenticación ess **WPA-PSK**.

Para configurar este tipo de seguridad, especifique una clave en el campo **Clave WPA previamente compartida** .

WPA2

Esta configuración de seguridad tiene un más seguro que la configuración WPA. Activa la autenticación **WPA2** y necesita que se indique la dirección IP y el secreto compartido para un servidor RADIUS. Los dispositivos clientes que se asocian al punto de acceso autónomo usando este SSID deben tener capacidad WPA2. El tipo de cifrado es **AES CCMP**, y los tipos de autenticación son **autenticación abierta con EAP** y **EAP de red**.

Configuration Assistant activa tanto la **Autenticación abierta con EAP** como la **Autenticación EAP de redes** para permitir que tanto los dispositivos clientes de Cisco como los que no son clientes de Cisco se asocien con el punto de acceso autónomo usando el mismo SSID para realizar la autenticación IEEE 802.1x.

Para configurar este tipo de seguridad:

PASO 1 Especifique la dirección IP del servidor RADIUS.

PASO 2 Especifique el secreto compartido que el punto de acceso autónomo usarñá para comunicarse con el servidor RADIUS.

WPA2-PSK

Seleccione esta configuración de seguridad cuando desee usar el cifrado WPA2 y no se tiene acceso a un servidor RADIUS. Necesita que el punto de acceso autónomo y el dispositivo cliente compartan el mismo WPA2-PSK. La clave puede tener entre 8 y 63 caracteres de largo. El tipo de cifrado es **AES CCMP**, y el tipo de autenticación es **WPA-PSK**.

Para configurar este tipo de seguridad, especifique una clave en el campo **Clave WPA2 previamente compartida** .

MAC

Seleccione esta configuración de seguridad cuando se desee autenticar dispositivos de clientes usando la autenticación basada en MAC.

No hay cifrado, y el tipo de autenticación es Autenticación abierta.

Para configurar este tipo de seguridad:

PASO 1 Especifique la dirección IP del servidor RADIUS.

PASO 2 Especifique el secreto compartido que el punto de acceso autónomo usarñá para comunicarse con el servidor RADIUS.

MAC y EAP

Seleccione esta configuración de seguridad cuando se desee autenticar dispositivos de clientes usando una combinación de autenticación EAP y autenticación basada en MAC. Los dispositivos de cliente que se asocian con el punto de acceso usando la autenticación abierta IEEE 802.11 primero intentan la autenticación MAC. Si tiene éxito la autenticación MAC, el dispositivo cliente se une a la red; si el cliente también está usando la autenticación EAP,éste intenta autenticarse usando EAP. Si la autenticación MAC falla, el punto de acceso espera que el dispositivo del cliente intente la autenticación EAP.

El tipo de cifrado es WEP dinámica y los tipos de autenticación son Autenticación abierta con EAP y Autenticación EAP.

Configuration Assistant activa tanto la **Autenticación abierta con EAP** como la **Autenticación EAP de redes** para permitir que tanto los dispositivos clientes de Cisco como los que no son clientes de Cisco se asocien con el punto de acceso autónomo usando el mismo SSID para realizar la autenticación 802.1x.

Para configurar este tipo de seguridad:

PASO 1 Especifique la dirección IP del servidor RADIUS.

PASO 2 Especifique el secreto compartido que el punto de acceso autónomo usarñá para comunicarse con el servidor RADIUS.

Ventana Resolución de VLAN invitada

Aparece la ventana Resolución deVLAN invitada si una VLAN invitada ya está configurada en un switch de la serie ESW500 y se abre la ventana WLAN (SSID) con el SR520 seleccionado como el host.

Haga clic en **Resolver** para crear la VLAN invitada en el SR520. Haga clic en Cancelar si no desea que CCA cree la VLAN invitada en el SR520.

Convertir a Punto de acceso liviano (LAP)

Esta ventana aparece cuando se selecciona **Configurar** > **Inalámbrica** > **Convertir a LAP** en la barra de funciones.

Se puede convertir un **Punto de acceso autónomo** en un **punto de acceso liviano**. Un punto de acceso liviano se asocia a un controlador LAN inalámbrico. El controlador administra las transacciones de control, configuración y firmware, como las autenticaciones 802.1x. Además, todo el tráfico de datos inalámbricos se canaliza a través del controlador.

Para convertir un punto de acceso autónomo en un punto de acceso liviano, seleccione y use la ventana Convertir a LAP. Consulte**Convertir a Punto de acceso liviano (LAP), página 235**). Se pueden seleccionar múltiples puntos de acceso autónomos y convertirlos al mismo tiempo.

CCA no admite la conversión de puntos de acceso LAP a AP autónomos. CCA no podrá administrar los puntos de acceso LAP convertidos a autónomos usando la interfaz de línea de comandos (CLI) de IOS de Cisco.

Esta tabla explica la configuración en la ventana de Convertir a LAP.

Configuración	Explicación
Dispositivo	Muestra los iconos de dispositivos y nombres de host.
Convertir	Muestra si el dispositivo está seleccionado para una **Conversión**.
Tipo de dispositivo	Muestra el tipo de dispositivo.
Versión actual	Muestra la versión actual de IOS de Cisco.
Recuperación de nombre de imagen	Muestra el nombre del archivo .tar de IOS de Cisco que usted proporcionó en la ventana Configuración de conversión. Sólo aparece el nombre del archivo; no la ruta.
Estado de la conversión	Muestra el estado de la conversión y los mensajes de progreso. Consulte la ventana Estado de la conversión para ver detalles.

Dirección IP	Muestra la configuración de dirección IP que se propporcionó en la ventana Configuración de conversión, ya sea estática o DHCP.
Su nombre de host	Muestra el nombre de host configurado en la ventana Configuración de conversión, ya sea Retener o No retener.

Sigas estos pasos para convertir los puntos de acceso autónomos en puntos de acceso livianos:

PASO 1 Descargue los archivos .tar de IOS de Cisco que desea usar para convertir el punto de acceso autónomo.

PASO 2 Seleccione uno o más puntos de acceso autónomos.

PASO 3 Haga clic en **Configuración de conversión**.

PASO 4 Complete la ventana Configuración de conversión y haga clic en **Aceptar** para guardar sus cambios. Consulte **Configuración de conversión, página 237**.

PASO 5 Marque la casilla **Convertir** al lado de cada dispositivo que desea convertir.

PASO 6 Haga clic en **Convertir** para iniciar el proceso de conversión.

La imagen actual se elimina y se descarga la nueva. Se puede guardar la imagen antigua usando la interfaz de línea de comandos (CLI).

PASO 7 Haga clic en **Estado** para mostrar la ventana Estado de conversión. Esta ventana muestra el progreso de la conversión. Consulte **Estado de la conversión, página 238**.

Cuando se completa el proceso de conversión, aparece un diálogo de confirmación. Los mensajes de estado indican cuáles puntos de acceso se convirtieron con éxito y cuáles no.

PASO 8 Todos los cambios de configuración se guardan automáticamente en la memoria flash. Después de un (1) minuto, los dispositivos son recargados y la nueva imagen comienza a funcionar. Luego puede cerrar la ventana Convertir a LAP.

Usted pierde conectividad a un dispositivo cuando lo recarga.

Configuración de conversión

Esta ventana aparece cuando usted selecciona un **Punto de acceso autónomo**, o más, en la ventana Convertir a LAP y hace clic en **Configuración de conversión**.

Seleccione **Dirección IP de DHCP** si desea que el controlador de WLAN asigne una nueva dirección IP al punto de acceso liviano después de la conversión.

Seleccione **Retener nombre de host** si desea retener el mismo nombre de host para el punto de acceso liviano después de la conversión.

En la lista **Modo**, seleccione **Estándar** para usar una imagen de conversión que se guarde localmente; de lo contrario, seleccione **Servidor TFTP remoto**.

Si seleccionó **Estándar**, indique el nombre del archivo de la imagen de conversión en el campo **Imagen de conversión**. Puede hacer clic en **Navegar** para encontrar el archivo.

Si seleccionó **Servidor TFTP remoto**:

PASO 1 En el campo **Imagen de conversión**, especifique la ruta completa y el nombre del archivo de la imagen de conversión.

PASO 2 En el campo **Dirección IP del servidor TFTP** , especifique la dirección IP de su servidor TFTP.

Para realizar conversiones de grupos, su servidor TFTP debe manejar múltiples solicitudes y sesiones simultáneamente.

PASO 3 En el campo **Nombre de dominio** , indique el nombre del dominio.

PASO 4 En el campo **Dirección IP de DNS** , especifique la dirección **DNS**.

PASO 5 Haga clic en **Aceptar** para guardar su configuración. Aparecen en la ventana Convertir a LAP.

Estado de la conversión

Esta ventana aparece cuando usted selecciona un **Punto de acceso autónomo**, o más, en la ventana Convertir a LAP y hace clic en **Estado**. La ventana muestra mensajes detallados a medida que se generan desde el punto de acceso autónomo durante una conversión.

Esta tabla explica los mensajes de estado de conversión.

Mensaje	Explicación
Haga clic en el botón **Configuración de conversión** para continuar	La ventana Configuración de conversión se debe completar antes de convertir el dispositivo.
Haga clic en el botón **Convertir** para actualizar el dispositivo.	Todos los parámetros se configuran para el dispositivo a convertir.
Determinación del tamaño total de la memoria flash.	El proceso de conversión verifica si hay suficiente espacio disponible para convertir el dispositivo.
Extracción del archivo de información desde el archivo de imagen .tar.	El archivo .tar de la imagen de IOS de Cisco está extrayendo el archivo de información.
Lectura del archivo de información del archivo de imagen .tar.	Configuration Assistant lee el archivo de información del archivo .tar de la imagen de IOS de Cisco para ver los detalles acerca de la imagen de IOS de Cisco.
Recarga iniciada para el dispositivo.	El dispositivo se recarga después de una conversión exitosa. Incluso después de completar la recarga, este mensaje aparece hasta que usted actualiza la ventana.
La conversión del dispositivo se completó con éxito.	Se completó exitosamente la conversión.
Fallo en la conversión del dispositivo.	Error en la conversión. Vea la ventana Detalles para obtener más información.

Mensaje	Explicación
Conversión de dispositivo en progreso.	La conversión de los dispositivos está en proceso.
La conversión del dispositivo se canceló.	Se canceló la conversión.
Cargando la imagen.	La imagen se carga al dispositivo.
Verificando la imagen IOS.	El dispositivo está verificando la imagen.

Si no hay espacio suficiente en el dispositivo para instalar la nueva imagen, aparece un mensaje con un enlace a la ventana Administración de archivos. Puede utilizar la ventana Administración de archivos para administrar los archivos del sistema y, si es necesario, eliminar las imágenes antiguas para liberar espacio para las nuevas imágenes.

Haga clic en **Aceptar** cuando termine en esta ventana.

Configuración del controlador de LAN inalámbrica

Los temas de esta sección abarcan los parámetros de configuración para los controladores de WLAN:

- **Configuración de interfaces inalámbricas para un controlador de WLAN, página 240**
- **Visualización de estado de clientes inalámbricos para un controlador de WLAN, página 242**
- **Configuración de usuarios de WLAN, página 243**
- **Proxy DHCP, página 250**
- **Tablero del controlador inalámbrico, página 250**
- **Configurar el servidor RADIUS para controladores de WLAN, página 252**

Configuración de interfaces inalámbricas para un controlador de WLAN

Si sus sistema incluye un controlador de WLAN inalámbrica, seleccione **Configurar** > **Interfaces Inalámbricas** en la barra de funciones.

Visión general

Se puede configurar interfaces inalámbricas dinámicas en un controlador de WLAN. las interfaces inalámbricas dinámicas son análogas a las VLNA para los clientes de LAN inalámbricas. Un controlador puede admitir hasta 8 interfaces dinámicas (VLAN).

Una interfaz inalámbrica tiene múltiples parámetros asociados a ella, incluyendo un identificador VLAN, puerto, dirección IP, máscarga de subred, gateway por defecto (para la subred IP) y un servidor DHCP.

Use esta ventana para ver todas las configuraciones de interfaces inalámbricas del controlador de WLAN y para configurar interfaces inalámbricas dinámicas (definidas por el usuario) en el controlador de WLAN.

Procedimientos

Esta tabla explica las columnas de la ventana Interfaces inalámbricas.

Columna	Explicación
Nombre	El nombre de la interfaz inalámbrica, incluyendo interfaces dinámicas y estáticas (administración, administrador AP y virtual)
VLAN	La VLAN asociada con la interfaz inalámbrica
Puerto	El número del puerto físico para la interfaz inalámbrica
Dirección IP	Dirección IP de la interfaz inalámbrica

Siga estos pasos para configurar una interfaz inalámbrica dinámica en el controlador de WLAN:

PASO 1 En la lista **Nombre de host**, seleccione el controlador de WLAN.

PASO 2 Para crear una interfaz, haga clic en **Crear** y complete la ventana Crear interfaz. Consulte **Crear interfaz, página 241**.

Un controlador puede admitir hasta 8 interfaces dinámicas.

Para modificar una configuración, seleccione el nombre de la interfaz inalámbrica, haga clic en **Modificar**, y use la ventana Modificar interfaz.

Para eliminar una configuración, seleccione el nombre de la interfaz inalámbrica y haga clic en Eliminar.

NOTA Puede modificar y eliminar sólo interfaces dinámicas. No puede eliminar o modificar interfaces estáticas.

Para guardar sus cambios y cerrar la ventana, haga clic en **Aceptar** en la ventana Interfaces inalámbricas.

Crear interfaz

Esta ventana aparece cuando se hace clic en **Crear** en la ventana Interfaces inalámbricas. Use la ventana para crear una interfaz inalámbrica.

PASO 1 En el campo **Nombre de la interfaz**, indique un nombre para la interfaz inalámbrica.

PASO 2 En el campo **ID de VLAN**, especifique la ID de VLAN que desea asociar con la interfaz inalámbrica.

PASO 3 En la lista **Puerto**, seleccione un puerto para la interfaz inalámbrica.

PASO 4 En el **campo Dirección IP**, especifique la dirección IP para la interfaz inalámbrica.

PASO 5 En la lista **Máscara de subred**, seleccione la máscara de subred para la interfaz inalámbrica.

PASO 6 En el campo **Dirección IP del gateway**, especifique la dirección IP del gateway por defecto.

PASO 7 En el campo **Dirección IP del servidor DHCP** , especifique la dirección IP del servidor DHCP.

PASO 8 Cuando termine con esta ventana, haga clic en **Aceptar** para guardar sus cambios y cerrar la ventana.

Modificar interfaces

Esta ventana aparece cuando se hace clic en **Modificar** en la ventana Interfaces inalámbricas. Use la ventana para modificar la configuración de una interfaz inalámbrica.

Siga estos pasos:

PASO 1 En el campo **ID de VLAN**, especifique la ID de VLAN que desea asociar con la interfaz inalámbrica.

PASO 2 En la lista **Puerto**, seleccione un puerto para la interfaz inalámbrica.

PASO 3 En el campo **Dirección IP**, especifique la dirección IP para la interfaz inalámbrica.

PASO 4 En la lista **Máscara de subred**, seleccione la máscara de subred para la interfaz inalámbrica.

PASO 5 En el campo **Dirección IP del gateway**, especifique la dirección IP del gateway por defecto.

PASO 6 En el campo **Dirección IP del servidor DHCP** , especifique la dirección IP del servidor DHCP.

PASO 7 Cuando termine con esta ventana, haga clic en **Aceptar** para guardar sus cambios y cerrar la ventana.

Visualización de estado de clientes inalámbricos para un controlador de WLAN

Para mostrar el estado de los clientes inalámbricos en el controlador de WLAN, use la ventana Clientes inalámbricos.

Esta table explica la información que se visualiza en las columnas de esta ventana.

Columna	Explicación
Dirección MAC	La dirección MAC del cliente.

Columna	Explicación
Estado	El estado de la conexión del cliente: ▪ Desocupada ▪ Pendiente ▪ Autenticada ▪ Asociada ▪ Activa ▪ Ahorro de energía ▪ Disociada ▪ Excluida ▪ Probando
Nombre de AP	Nombre del punto de acceso liviano del cliente
SSID	El SSID del cliente
Radio	El tipo de cliente: ▪ 802.11a ▪ 802.11 b ▪ 802,11g
Autenticada	Estado de autenticación del cliente (sí o no)

Para cerrar la ventana, haga clic en **Aceptar**.

Configuración de usuarios de WLAN

Se puede configurar usuarios inalámbricos en el controlador de WLAN. También se puede configurar la autenticación y el inicio de sesión en Internet.

Los usuarios inalámbricos pueden ser invitados o no (por ejemplo, empleados).

Los usuarios invitados tienen acceso a Internet y a la propia red del invitado sin comprometer la seguridad de su red. El acceso del usuario invitado se configura con una fecha de vencimiento.

Los usuarios que no son invitados tienen acceso seguro a la red. No hay fecha de vencimiento para este tipo de acceso de usuario.

Use esta ventana para configurar usuarios inalámbricos en el controlador de WLAN o para ver la configuración de los usuarios inalámbricos que se realizó en el controlador de WLAN.

Esta tabla explica las columnas en el área Usuarios de redes inalámbricas.

Columna	Explicación
Nombre de usuario	Nombre del usuario inalámbrico.
Usuario invitado	Estado de usuario invitado (sí o no).
SSID	Nombre del SSID.
Hora final	La fecha de vencimiento del acceso del usuario invitado.
Descripción	Descripción del usuario inalámbrico.

Siga estos pasos para configurar usuarios inalámbricos para el controlador de WLAN:

PASO 1 En la lista **Nombre de host**, seleccione el controlador de WLAN.

PASO 2 Para crear un usuario invitado o no invitado, haga clic en **Crear**, y complete la ventana Crear usuario de WLAN. Consulte **Crear usuarios de WLAN, página 245**.

PASO 3 Para guardar sus cambios y cerrar la ventana, haga clic en **Aceptar** en la ventana Usuarios de WLAN.

Para modificar un usuario inalámbrico, seleccione el nombre del usuario, haga clic en Modificar, y use la ventana Modificar usuario de WLAN.

Para eliminar un usuario inalámbrico, seleccione su nombre de usuario y haga clic en **Eliminar**.

Los usuarios invitados se eliminan automáticamente de la lista Usuarios de redes inalámbricas cuando se abre la ventana Usuarios de WLAN y se ha cumplido el tiempo del usuario invitado. Si ya está abierta la ventana Usuarios de WLAN cuando se termina el tiempo del usuario invitado y se intenta modificar al usuario invitado, éste se eliminará de la lista Usuarios de redes inalámbricas. Haga clic en **Crear** para crear un nuevo Usuario invitado.

Para configurar una oágina de inicio de sesión para los usuarios inalámbricos, haga clic en **Configurar** en el área Inicio de sesión en Internet. Consulte **Inicio de sesión en Internet, página 248**.

Crear usuarios de WLAN

Esta ventana aparece cuando se hace clic en **Crear** en la ventana Usuarios de WLAN. Use la ventana para crear un nuevo usuario inalámbrico.

Visión general

Se puede configurar usuarios inalámbricos en el controlador de WLAN. También se puede configurar la autenticación y el inicio de sesión en Internet.

Los usuarios inalámbricos pueden ser invitados o no (por ejemplo, empleados).

Los usuarios invitados tienen acceso a Internet y a la propia red del invitado sin comprometer la seguridad de su red. El acceso del usuario invitado se configura con una fecha de vencimiento.

Los usuarios que no son invitados tienen acceso seguro a la red. No hay fecha de vencimiento para este tipo de acceso de usuario.

Procedimientos

Siga estos pasos:

PASO 1 En el campo **Nombre de usuario**, especifique un nombre para el usuario inalámbrico. Es posible especificar hasta 24 caracteres alfanuméricos.

PASO 2 En el campo **Contraseña**, especifique una contraseña para el usuario inalámbrico. Es posible especificar hasta 24 caracteres alfanuméricos.

PASO 3 En el campo **Confirmar contraseña**, indique la contraseña nuevamente.

PASO 4 En el campo **Descripción**, especifique una descripción para el usuario inalámbrico.

PASO 5 Si el usuario inalámbrico no es un usuario invitado, siga estos pasos:

a. Desmarque la casilla **Usuario invitado**.

b. Seleccione un SSID de la lista de SSID. Sólo aparecen SSID que se configuren con seguridad Web-Auth, WEP, WPA1-PSK, ó WPA2-PSK.

Si necesita crear un SSID, haga clic en **Agregar SSID** (definido previamente) para abrir la ventana Agregar SSID (definido previamente). Consulte **Agregar SSIC, página 247**.

PASO 6 Si el usuario inalámbrico es un usuario invitado, siga estos pasos:

a. Marque la casilla **Usuario invitado**.

b. Seleccione un SSID de la lista de SSID. Sólo aparecen SSID que se configuren con seguridad Web-Auth.

Si necesita crear un SSID, haga clic en **Agregar SSID** (definido previamente) para abrir la ventana Agregar SSID (definido previamente). Consulte **Agregar SSIC, página 247**.

PASO 7 En el área **Hora final**, indique la fecha de vencimiento, seleccionando el año, mes, día, hora y minuto. La fecha de vencimiento máxima para un usuario invitado es de 30 días desde la fecha actual.

Cuando termine con esta ventana, haga clic en **Aceptar** para guardar sus cambios y cerrar la ventana.

Modificar usuarios de WLAN

Esta ventana aparece cuando se hace clic en **Modificar** en la ventana Usuarios de WLAN. Use esta ventana para modificar la configuración de los usuarios inalámbricos.

Siga estos pasos:

PASO 1 En el campo **Contraseña**, especifique una contraseña para el usuario inalámbrico. Es posible especificar hasta 24 caracteres alfanuméricos.

PASO 2 En el campo **Confirmar contraseña**, indique la contraseña nuevamente.

PASO 3 En el campo **Descripción**, especifique una descripción para el usuario inalámbrico.

PASO 4 En la lista **SSID**, seleccione un SSID.

PASO 5 Si el usuario inalámbrico es un usuario invitado, modifique la fecha de vencimiento en el área **Hora final** seleccionando el año, mes, día, hora y minuto. La fecha de vencimiento máxima para un usuario invitado es de 30 días desde la fecha actual.

PASO 6 Cuando termine con esta ventana, haga clic en **Aceptar** para guardar sus cambios y cerrar la ventana.

Agregar SSIC

Esta ventana aparece cuando hace clic en **Agregar SSID** en el área SSID de la ventana Crear usuario de WLAN. Úsela para aplicar la configuración de SSID definida al controlador de WLAN.

Configuration Assistant configura la correspondiente VLAN y SSID con el tipo de seguridad establecido. Una vez que haya aplicado la configuración de SSID definida previamente al controlador de WLAN, puede modificar o eliminar la correspondiente WLAN de la ventana WLAN (SSID). También puede modificar o eliminar la VLAN correspondiente de la ventana WLAN.

Siga estos pasos para agregar un SSID:

PASO 1 Seleccione un tipo de red inalámbrica en el área Selección de WLAN. Las opciones son:

- Datos de empleados (usando Web-Auth y WPA1-PSK)
- Datos de voz (usando Web-Auth y WPA2-PSK)

Si está configurando un usuario invitado, se selecciona la opción Invitado (usando Web-Auth).

PASO 2 Dependiendo de la selección de WLAN, indique la siguiente información:

- **ID de VLAN (2-1000)—**Indique la ID de la VLAN.
- **Nombre de VLAN—**Para las redes de datos, acepte el nombre predefinido o indique un nombre diferente para la VLAN. Para las redes de voz o invitadas, este campo se configura con un nombre de VLAN predefinido que se basa en su selección de WLAN.
- **Dirección IP—**Indique una dirección IP para la VLAN.
- **Máscara de subred—**Seleccione la máscara de subred para la VLAN.
- **Dirección IP del gateway**-Especifique la dirección IP del gateway por defecto.

- **Dirección IP del servidor DHCP** -Especifique la dirección IP del servidor DHCP.
- **SSID**—Acepte el SSID por defecto (basado en el nombre de la empresa y su selección de WLAN), o indique un SSID diferente de hasta 32 caracteres alfanuméricos.
- **Clave previamente compartida WPA1** (para redes de datos) o **Clave previamente compartida WPA2** (para redes de voz)—Indique una clave de entre 8 y 63 caracteres de largo.

PASO 3 Cuando termine con esta ventana, haga clic en **Aceptar** para guardar sus cambios y cerrar la ventana.

Inicio de sesión en Internet

Esta ventana aparece cuando se hace clic en **Configurar** en la área Inicio de sesión en Internet de la ventana Usuarios de WLAN. Úsela para personalizar el contenido y apariencia de la página de inicio de sesión en Internet para los usuarios de WLAN.

Visión general

La página de inicio de sesión se presenta a los usuarios de Internet la primera vez que acceden a una WLAN con autenticación por Internet activada. Cisco entrega una página de inicio de sesión en Internet por defecto que puede modificarse con cualquier editor de HTML basado en texto. Sin embargo, los campos Nombre de usuario y Contraseña no deben cambiarse y debe conservarse el método Enviar. Una vez que se ha creado la página de inicio de sesión en Internet, debe convertirse en un archivo .tar que contenga el código de la página y cualquier imagen que se desee.

Procedimientos

Siga estos pasos para configurar la página de inicio de sesión.

PASO 1 En la lista **Nombre de host**, seleccione el controlador de WLAN.

PASO 2 En el área **Autenticación en Internet**, seleccione**Interno** o **Personalizado**.

PASO 3 Si se selecciona **Interno**, siga estos pasos:

a. En el área de Logo de Cisco, seleccione Mostrar para ver el logo de Cisco en la página de inicio de sesión, o seleccione Ocultar para ocultar el logo. Por defecto, la selección es Mostrar.

b. En el campo Redirigir a URL después de inicio de sesión, indique una URL a la que se dirigirá el usuario después de iniciar sesión. Indique la URL usando el formato www.nombredelaempresa.com con hasta 254 caracteres.

c. En el campo Encabezado, indique el encabezado o resumen del encabezado de inicio de sesión, hasta 127 caracteres. El título por defecto es "Bienvenido a la red inalámbrica de Cisco."

d. En el campo Mensaje, indique un mensaje de texto, de hasta 2047 caracteres. El mensaje por defecto es "Cisco se complace en ofrecer la infraestructura de red LAN inalámbrica para la red. Por favor, identifíquese y poner su espacio aéreo a trabajar."

Haga clic en **Dejar por defecto** para usar la configuración por defecto.

PASO 4 Si se selecciona **Personalizado**, siga estos pasos:

a. En el campo Dirección IP del servidor TFTP, indique la dirección IP del servidor TFTP en que existe el archivo de autenticación en Internet personalizado.

El servidor TFTP no puede ejecutarse en el mismo computador que el WCS de Cisco, porque el WCS de Cisco y el servidor TFTP usan el mismo puerto de comunicación.

b. En el campo **Máximo de intentos**, indique el número de intentos que el controlador de WLAN realiza para cargar el archivo de autenticación en Internet desde el servidor TFTP en caso de fallos. El valor por defecto es 3.

c. En el campo **Límite de tiempo** (segundos), indique el período del límite de timepo (en segundos). Si el controlador de WLAN no puede comenzar la descarga del archivo dentro de este período, no se produce la carga.

d. En el campo **Ruta de archivo**, indique la ruta del archivo de autenticación en Internet del servidor TFTP. El valor, por defecto, es barra (/).

e. En el campo **Nombre de archivo**, indique el nombre del archivo que se va a transferir.

f. Haga clic en **Descargar** para descargar el archivo de inicio de sesión personalizado.

PASO 5 Cuando se hace clic en **Aceptar** o **Aplicar**, la descarga comienza y se aplica el archivo de inicios de sesión personalizado al dispositivo.

Proxy DHCP

Para configurar un proxy DHCP, seleccione **Configurar** > **proxy DHCP** en la barra de funciones.

Un proxy DHCP ayuda a los clientes inalámbricos a obtener una dirección IP del servidor DHCP. El controlador de WLAN recibe la solicitud de descubrir DHCP del cliente inalámbrico y envía la solicitud al servidor DHCP en nombre del cliente. Cuando se active el procy DHCP, el controlador de WLAN trabaja entre el cliente inalámbrico y el servidor DHCP hasta que el cliente reciba una dirección IP.

Se puede activar el proxy DHCP si se configuró una dirección del servidor DHCP en todas las VLAN definidas por el usuario para este dispositivo.

Para activar el proxy DHCP, siga estos pasos.

PASO 1 Seleccione un dispositivo para configurar de la lista **Nombre de host**.

PASO 2 Marque la casilla **Activar proxy DHCP**.

PASO 3 Haga clic en **Aceptar** para guardar sus cambios y cerrar la ventana.

Tablero del controlador inalámbrico

Si desea información para todos los controladores de WLAN en la comunidad, (por ejemplo, el estado del sistema controlador de WLAN, el estado de la 802.11 b/g radios, el número de clientes que están asociados con un SSID), seleccionar para abrir el Interfaz del controlador inalámbrico. Muestra un intervalo amplio de información del controlador de WLAN, como:

- Resumen del sistema
- Detalles y características de punto de acceso
- Estadísticas del controlador de WLAN

Muestra un intervalo amplio de estadísticas en estas fichas: Sistema, Resumen de AP, WLAN, Estadísticas de WLC y Estadísticas de AP. Para actualizar las estadísticas, haga clic en **Actualizar**.

Esta tabla explica los datos de la sección Sistema.

Columna	Explicación
Nombre del controlador	Nombres de los controladores.
Tiempo activo	La cantidad de tiempo que ha transcurrido desde que se reinició por última vez el controlador de WLAN.
Temperatura	Temperatura interna del chasis.
CPU	Uso total de la CPU del controlador de WLAN.
Memoria	Uso total de la memoria del controlador de WLAN.

Esta tabla explica los datos de la sección Resumen de AP.

Columna	Explicación
Nombre del controlador	Nombres de los controladores.
Radios 802.11b/g	Estado de las radios (Encendidas y Apagadas).
Estado de AP	Estado de los puntos de acceso (Encendidos y Apagados).

Esta tabla explica los datos de la sección WLAN.

Columna	Explicación
Nombre de WLAN (Nombre del controlador)	Nombres SSID de los controladores.
Clientes	Número de clientes asociados con este SSID.

Esta tabla explica los datos de la sección Estadísticas de WLC. Puede seleccionar mostrar los datos en números totales o en porcentajes.

Columna	Explicación
Nombre del controlador	Nombres de los controladores.
Paquetes recibidos sin errores	Número total o porcentaje de los paquetes recibidos.
Paquetes recibidos rechazados	Número total o porcentaje de los paquetes recibidos y rechazados.
Paquetes transmitidos sin errores	Número total o porcentaje de los paquetes enviados.
Paquetes transmitidos rechazados	Número total o porcentaje de los paquetes enviados y rechazados.

Esta tabla explica los datos de la sección Estadísticas de AP.

Columna	Explicación
Nombre de AP (Nombre del controlador)	Puntos de acceso asociados con los controladores de WLAN.
Cuenta de tramas transmitidas	Número total de tramas enviadas.
Cuenta de transmisiones fallidas	Número total de tramas cuyo envío fracasó.

Configurar el servidor RADIUS para controladores de WLAN

Aparece la ventana Configurar los servidores RADIUS cuando se hace clic en **Configurar** en el área Servidores RADIUS de la ventana WLAN (SSID) para un controlador de WLAN.

En esta ventana se puede ver la configuración del servidor RADIUS para el controlador de WLAN y configurar hasta dos servidores RADIUS para el controlador de WLAN. Esta tabla explica las columnas de la ventana.

Configuración	Descripción
Dirección IP	Dirección IP del servidor RADIUS.
Puerto Auth	Número del puerto de autenticación RADIUS.
Prioridad	Prioridad del servidor RADIUS. Especifica el orden en que se usan los servidores si uno de ellos no puede ubicarse.
Estado	Estado del servidor RADIUS, Activado o Desactivado.

Para configurar los servidores RADIUs para el controlador WLAN, siga estos pasos.

PASO 1 En la lista Nombre de host, seleccione el controlador de WLAN.

PASO 2 Haga clic en **Crear** y complete la configuración en la ventana Crear servidor RADIUS. Consulte **Ventana Crear servidor RADIUS**.

Para cambiar el estado del servidor RADIUS, seleccione su dirección IP, haga clic en **Modificar** y complete la configuración en la ventana Crear servidor RADIUS. Consulte **Ventana Modificar servidor RADIUS**.

Para eliminar un servidor RADIUS configurado, seleccione la dirección IP de dicho servidor y haga clic en **Eliminar**.

Para guardar sus cambios y cerrar la ventana, haga clic en **Aceptar** en la ventana Servidor RADIUS.

Ventana Crear servidor RADIUS

Esta ventana aparece cuando se hace clic en **Crear** en la ventana Configurar servidor RADIUS. Use esta ventana para especificar la configuración del servidor RADIUS.

Siga estos pasos.

PASO 1 En el campo **Dirección IP**, especifique la dirección IP del servidor RADIUS.

PASO 2 En el campo **Puerto Auth**, indique el número del puerto de autenticación RADIUS. El número de puerto de autenticación por defecto es 1812.

PASO 3 En el campo **Clave secreta (ASCII)** , indique la clave secreta compartida que usará el controlador de WLAN para comunicarse con el servidor RADIUS.

PASO 4 En el campo **Confirmar clave secreta**, repita la clave secreta compartida.

PASO 5 En la lista **Clave de prioridad del servidor**, seleccione la prioridad del servidor.

NOTA Cada servidor RADIUS debe usar un número de prioridad diferente.

PASO 6 En la lista **Estado de administrador**, seleccione Activado o Desactivado.

PASO 7 Haga clic en **Aceptar** para guardar sus cambios y cerrar la ventana.

Ventana Modificar servidor RADIUS

Esta ventana aparece cuando se hace clic en **Modificar** en la ventana Configurar servidor RADIUS. Use la ventana para cambiar el estado de un servidor RADIUS.

Siga estos pasos:

PASO 1 En la lista **Estado de administrador**, seleccione Activado o Desactivado.

PASO 2 Haga clic en **Aceptar** para guardar sus cambios y cerrar la ventana.

8

Funciones de seguridad

Esta sección cubre la configuración de las siguientes fuciones de seguridad avanzadas:

- **Traducción de direcciones de la red (NAT)**
- **Servidor VPN**
- **Auditoría de seguridad**
- **Firewall y DMZ**
- **Configuración de seguridad de red (Switches CE520)**
- **VPN SSL**
- **Sistema de prevención de intrusiones (IPS)**
- **Filtro de URL (serie SR500)**

Traducción de direcciones de la red (NAT)

Para activar o desactivar la traducción de direcciones de la red (NAT) seleccione **Configurar** > **Seguridad** > **NAT** en la barra de funciones.

En esta ventana, se puede:

- Activar o desactivar la Traducción de direcciones de la red (NAT)
- Configurar el mapeo de puertos
- Configurar el reenvío de puertos

NOTA: La interfaz de usuario de la ventana NAT y su configuración son diferentes, basados en cómo se asignan las direcciones IP.

Para obtener información acerca de las funciones y configuración NAT, consulte las siguientes secciones:

- Visión general
- Ventana NAT (Direcciones IP asignadas a través de DHCP)
- Ventana NAT (IP estática o PPPoE con IP estática)

Visión general

Cuando se activa en una interfaz, Traducción de direcciones de la red (NAT) mapea las direcciones IP privadas de su LAN a una dirección IP de red pública desde un grupo de direcciones IP de redes públicas registradas.

Es necesaria una dirección IP pública válida, registrada y globalmente única para acceder a Internet. Por lo general, una organización no posee suficientes direcciones IP públicas para asignar una dirección IP pública y única a cada cliente de la organización que necesite acceso a Internet. Sin NAT, su conjunto de direcciones IP públicas se agotaría. La estructura interna de su LAN también quedaría expuesta a cualquier cliente de la red pública. NAT le permite utilizar una dirección IP pública para entregar acceso a Internet a muchos de los clientes de su LAN.

Copn Configuration Assistant, se mapea la dirección IP pública y única asignada a la interfaz de su WAN para múltiples direcciones IP privadas.

Es más fácil que un cliente no autorizado ataque su red si dicho cliente puede determinar la topología de su red utilizando sus direcciones IP de la red. NAT esconde sus direcciones IP privadas de la Internet. Si un atacante no puede adivinar la estructura de su LAN utilizando las direcciones IP, es mucho más difícil acceder a su red sin permiso.

In some cases—for example, when you configure a UC500 with a SIP trunk behind an SR500 secure router—NAT entries are created automatically by CCA.

NOTA NAT sólo admite interfaces de Ethernet de Capa 3. No admite interfaces de puertos de switch de nivel 2. Cuando activa NAT en una interfaz externa (no fiable), todas las demás interfaces calificadas se seleccionan en forma automática como interfaces internas (fiables).

NAT estática y NAT dinámica

La NAT estática funciona con las direcciones IP mapeadas estáticamente entre sí. Es decir, el administrador puede establecer un mapeo uno a uno entre las direcciones IP privadas y las públicas. Las traducciones estáticas se usan generalmente para permitir el acceso a un dispositivo en particular por medio de las NAT. Por ejemplo, si una red tiene un servidor DNS interno que necesite

comunicarse con un servidor DNS externo, el administrador configurará una traducción estática para activar dicha conectividad. Por ende, las NAT permiten que el tráfico pase entre estas direcciones estáticamente conocidas, pero traducidas.

Como alternativa, las NAT dinámicas mapean las direcciones IP privadas hacia las públicas. Las NAT dinámica usan un conjunto de direcciones públicas y las asigna en forma al azar (el primero en llegar recibirá asignaciones primero). Cuando un host con direcciones IP privadas solicita acceso a Internet, las NAT dinámicas seleccionan una dirección IP del conjunto que no estén en uso por parte de otro host. Las NAT dinámicas son útiles cuando menos direcciones están disponibles que el número real de host que se deben traducir.

Ventana NAT (Direcciones IP asignadas a través de DHCP)

Seleccione un dispositivo en el que desee activar NAT de la lista **Nombre del host**.

Para activar NAT, seleccione una interfaz_ externa (no fiable) de la lista **Interfaz externa**. Haga clic en **Detalles** para ver información acerca de la interfaz externa seleccionada.

Para crear una entrada para cada asignación de puerto, siga estos pasos:

PASO 1 Para agregar una entrada a la ventana NAT, haga clic en **Agregar**.

PASO 2 Seleccione una aplicación de la lista desplegable del campo Aplicación:

- Servidor web
- Servidor Web seguro
- Servidor de correo eectrónico
- FTP
- SSH
- SFTP
- Otro (TCP)
- Otro (UDP)

PASO 3 En el campo **Dirección Interna** , especifique una dirección IP que el servidor utilice en su red interna. Se trata de una dirección IP que no puede utilizarse, externamente, en Internet.

PASO 4 En el campo **Puerto interno**, especifique un núimero de puerto para el dispositivo interno, que sea el número de puerto que el servidor utilice para aceptar solicitudes de servicio desde la red interna.

PASO 5 En el campo **Puerto externo**, especifique un número de puerto que NAT vaya a utilizar para esta traducción. El número del puerto que utiliza el servidor para aceptar solicitudes de servicio desde Intenet.

Para aumentar la seguridad agregando un firewall, haga clic en **Servicio de firewall** y utilice la ventana Firewall. Consulte **Firewall, página 271** para esta configuración.

PASO 6 Haga clic en **Aceptar** o **Aplicar**.

Para eliminar una entrada de asignación de puertos, siga estos pasos:

PASO 1 Seleccione una entrada en la ventana.

PASO 2 Haga clic en **Eliminar**.

PASO 3 Para guardar sus cambios y cerrar la ventana, haga clic en **Aceptar**.

Se puede eliminar la configuración NAT para un dispositivo que esté detrás de otro dispositivo NAT en una red completamente enrutada. Por ejemplo, cuando se conecta un UC500 detrás de un router seguro de la serie SR500, se puede eliminar la configuración NAT del UC500.

Para eliminar toda la configuración NAT, siga estos pasos:

PASO 1 Haga clic en **Eliminar configuración NAT**.

Si hay entradas en la tabla IP, se muestra una ventana que advierte que si se continúa, se eliminarán los parámetros de la configuración NAT. Haga clic en **Aceptar** para cerrar el diálogo emergente y continuar.

PASO 2 En la ventana principal de NAT, haga clic en **Aceptar**.

Ventana NAT (IP estática o PPPoE con IP estática)

Los controles de la pantalla NAT estática IP se activan sólo cuando se asigna una dirección IP o PPEoE a la conexión a Internet (Interfaz de WAN).

El conjunto NAT debe provisionarse primero antes de agregar entradas a la mesa de mapeo NAT estático.

- **Crear Conjunto NAT**
- **Mapeo NAT estático**

Crear Conjunto NAT

Las direcciones IP para el conjunto NAT las entrega el Proveedor de servicios de Internet (ISP). Pueden agregarse hasta 10 entradas de conjuntos NAT.

Los usuarios no pueden indicar una dirección IP hacie el conjunto NAT que usa la interfaz WAN.

Crear una entrada para el conjunto NAT

PASO 1 Para crear una entrada de conjunto NAT, haga clic en el botón **Crear** que se ubica al lado de la table Conjunto NAT. Esto iniciará una nueva ventana etiquetada como Crear conjunto NAT.

PASO 2 Escriba un nombre en el campo **Nombre del conjunto**.

PASO 3 Escriba la dirección IP o haga clic en el **Intervalo específico de direcciones** y escriba el intervalo de direcciones IP.

NOTA: La dirección de red usada en el conjunto NAT debe estar en la misma subred que la entregada para la interfaz WAN.

PASO 4 Haga clic en **Aceptar**.

PASO 5 Luego de provisionar el conjunto NAT, haga clic en **Aplicar**, o en **Aceptar** para aplicar la configuración. Ello instalará el conjunto NAT y agregará las direcciones IP como una IP secundaria a la interfaz WAN.

Eliminar entrada del conjunto NAT

PASO 1 Para eliminar una entrada del conjunto NAT desde la table de conjuntos NAT, seleccione la entrada del conjunto deseado, y haga clic en el botón **Eliminar** ubicado al lado de la tabla de conjuntos NAT.

Esto eliminará todos los mapeos NAT estáticos que usan las direcciones IP configuradas para ese conjunto.

PASO 2 Haga clic en **Aplicar** o en **Aceptar**.

NOTA: Las direcciones IP usadas en un conjunto no pueden usarse para otro conjunto. Además, cada nombre de conjunto debe ser único.

Mapeo NAT estático

Las siguientes pautas se aplican a la creación de mapeos NAT estáticos:

- Cada par de direcciones IP debe ser único. Si una dirección IP interna o externa y un puerto se usan en un mapeo, entonces, la misma dirección IP no puede usarse para crear otro mapeo que no especifique un puerto. Por ejemplo, si el puerto interno 192.168.10.10:80 se mapea hacia 171.71.236.176:80, no se puede mapear también 192.168.10.10 hacia 171.71.236.175 ni 192.168.10.15 hacia 171.71.236.176
- Un mapeo NAT puede consistir en una dirección IP por sí misma o en una dirección IP con un número de puerto. Los números de puertos TCP/UDP bien conocidos se muestran en el camp Puerto interno/externo. Se puede escribir un número de puerto si no se muestra ninguno.
- Uda dirección IP interna o externa y un puerto que se usen para un mapeo no pueden usarse en mapeos a ninguna otra dirección IP ni a otro puerto. Por ejemplo, si el puerto interno 192.168.10.10:80 se mapea hacia el puerto externo 171.71.236.178:80, no se puede mapear también 192.168.10.10:80 hacia 171.71.236.176:80 ni 192.168.10.15:80 hacia 171.71.236.178:80.
- No se puede crear un mapeo estático usando sólo la dirección IP de WAN, pero se puede crear un mapeo usando la dirección IP de WAN con un puerto.

PASO 1 Para provisionar el mapeo NAT estático, haga clic en el botón **Crear** que se ubica al lado de la tabla Mapeo NAT estático.

PASO 2 Mapeo de direcciones IP internas y externas:

a. Escriba la dirección IP interna deseada en el campo **IP interna**.

b. Escriba la dirección IP registrada externamente en el campo **IP externa**.

PASO 3 Haga clic en **Aceptar**. Ello lo llevará de vuelta a la ventana NAT principal.

PASO 4 Haga clic en **Aceptar** o **Aplicar**.

Servidor VPN

Para configurar la configuración del servidor VPN, seleccione **Configurar** > **Seguridad** > **VPN** en la barra de funciones.

PRECAUCIÓN Cisco no recomiendas que se configure el servidor VPN en una conexión WAN remota. Si se interrumpe la conexión a la WAN, fallará la operación y el sistema se volverá inutilizable.

Visión general

Una Red privada virtual (VPN) permite que un cliente remoto tenga acceso a la red corporativa.

Una VPN es necesaria en las siguientes circunstancias:

- Se necesita acceder a la red SBCS desde una computadora remota fuera del firewall de la red.
- Se desea utilizar CCA para administrar un dispositico SBCS remoto a través de Internet.

Puede autorizar un dispositivo de VPN remota para que reciba políticas IPsec enviadas por el servidor de VPN. También puede configurar un servidor VPN para que envíe políticas IPsec a un dispositivo VPN remoto.

Cuando autoriza que los clientes VPN remotos reciban políticas de un servidor VPN, los usuarios finales pueden solicitar una conexión a su red corporativa por medio de un túnel VPN ingresando una contraseña. Cuando se necesita una conexión y el usuario remoto final está autenticado, un servidor CPN le envía los

parámetros a este cliente remoto. De lo contrario, al usuario se le solicitará que especifique manualmente los parámetros IPsec para configurar el túnel VPN. Los dispositivos VPN remotos incluyen routers IOS de Cisco, dispositivos de seguridad adaptativos de Cisco y clientes VPN de Cisco.

Un *grupo* VPN es un grupo de clientes VPN que comparten la misma información y configuración de autenticación. Las claves previamente compartidas o certificados digitales se utilizan para autenticas al cliente en un grupo. Las políticas de grupo pueden configurarse en la base de datos del router local o en un servidor externo tal como RADIUS o ambos, un servidor local y uno externo.

Se puede configurar una clave previamente compartida que autentica un cliente remoto. La clave previamente compartida mejora la seguridad de las comunicaciones entre el dispositivo remoto que recibe las políticas IPSec y un servidor. La clave previamente compartida del dispositivo remoto debe coincidir con la clave previamente compartida del servidor VPN.

NOTA El número máximo de conexiones de VPN simultáneas que permite CCA para las plataformas UC520 y UC540 es de 10. Para las plataformas UC560, se permiten hasta 20 conexiones de VPN simultáneas. Las conexiones de VPN que se utilicen para EZVPN, VPN SSL, Administrador de múltiples sitios, y para las VPN de teléfonos SPA525G se incluyen en este total.

Acceso a Internet — Túnel VPN

El acceso a internet puede lograrse por medio del túnel VPN. La seguridad de la conexión es mayor, porque se tiene protección VPN entre el cliente y el servidor. Los datos relacionados con Internet se desplazan a través del túnel hasta el servidor, donde se producen las comunicaciones con Internet, entregando las protecciones configuradas en el cliente y el servidor. Esto se compara con División de arquitectura de túneles, donce las comunicaciones por Internet se envían y reciben fuera del túnel VPN, sólo dependiendo de las protecciones configuradas en el cliente.

Acceso a Internet — División de túneles

Cuando se active división de túneles en una red remota, las comunicaciones del cliente con los dispositivos locales o de Internet con otras redes quedan cifradas. Los datos sólo se cifran cuando el usuario final está comunicándose con un subred protegida, típicamente, la red corporativa. Ello reduce el tiempo de procesamiento del dispositivo y mejora el rendimiento de la red.

Por ejemplo, un usuario de teletrabajo utiliza una PC cliente VPN para acceder a la red corporativa por medio de un router que entrega conectividad desde la ubicación del usuario por medio de Internet hasta la red corporativa utilizando un túnel VPN. Sin embargo, también podría haber otras PC en la ubicación del usuario

de teletrabajo que no sean parte de la red corporativa y no se les debe permitir acceso a la VPN. Ejemplos típicos de ello serían las PC utilizadas por el cónyuge o hijos del usuario. Estas PC necesitan tener acceso a Internet, y es probable que los usuarios utilizar el router del usuario de teletrabajo para evitar instalar una segunda conexión de banda ancha en el mismo hogar. El túnel IPsec puede estar activo en todo momento y utilizar IEEE 802.1x para autenticar a los usuarios corporativos que intenten obtener acceso desde el sitio remoto. Un servidor RADIUS en las oficinas corporativas centrales contiene la base de datos de los usuarios corporativos. Debido a que el túnel siempre estÃ¡ disponible, el router remoto puede consultar con la base de datos para confirmar las credenciales 802.1x (nombre de usuario y contraseña) del usuario de teletrabajo para permitirle acceso a la VPN y, no obstante, excluir a todos los demás.

PRECAUCIÓN: La división de túneles puede presentar, potencialmente, un riesgo a la seguridad cuando esté configurada. Debido a que los clientes VPN tienen acceso no seguro a la Internet, los clientes CPN pueden quedar expuestos a un ataque. Dicho ataque podría lograr acceso a la LAN corporativa por medio del túnel IPsec utilizando la identidad del cliente VPN.

Procedimientos

Comience seleccionando un dispositivo para configurar de la lista **Nombre de host**.

Configure los parámetros en cada una de estas fichas en la ventana Servidor VPN:

- **Configuración del servidor**
- **Cuentas de usuario**
- **Acceso a la red**
- **Perfil VPN**

Configuración del servidor

Para activar un servidor VPN, configure las políticas y configuración del servidor VPN como se describe en la siguiente tabla.

Una vez que haya finalizado la configuración del servidor, haga clic en **Aplicar** para aplicarla, luego, en **Aceptar** para salir de la ventana del Servidor VPN o haga clic en las fichas Cuentas de usuario o Acceso a la red para seguir con la configuración de VPN.

Configuración	Descripción
Interfaz(ces) del servidor VPN	Seleccione o visualice las interfaces del Servidor VPN. Si sólo se muestra una interfaz, este parámetro es de sólo lectura.
Grupo VPN Configure el grupo VPN Un *grupo* VPN es un grupo de clientes VPN que comparten la misma información y configuración de autenticación.	
Nombre del grupo VPN	Campo de sólo lectura. El nombre del grupo VPN por defecto que utiliza Configuration Assistant es EZVPN_GROUP_1.
Conexiones máximas	Cantidad máxima de clientes del grupo VPN que pueden conectarse al Servidor VPN.
Claves previamente compartidas	Especifique la clave previamente compartida para autenticar a los clientes y dispositivos remotos de VPN, luego, vuelva a especificarla para confirmar. La clave puede contener desde 8 hasta 127 caracteres alfanuméricos. No se admiten espacios ni signos de interrogación (?).
Intervalo IP de VPN remota	Especifique una dirección IP de inicio y una de término para especificar un intervalo de direcciones IP desde las que se asigna una dirección IP a un usuario. Pueden especificarse hasta 10 direcciones IP para las plataformas UC520 ó UC540; hasta 20 direcciones IP pueden especificarse para las plataformas UC560.
DNS	
DNS principal	Especifique la dirección IP del servidor DNS principal para el servidor VPN.
DNS secundario	Opcional. Especifique la dirección IP del servidor DNS secundario para el servidor VPN.

Para eliminar un servidor VPN, siga estos pasos:

PASO 1 Haga clic en **Eliminar**.

Aparecerá una ventana, advirtiéndole que si continúa, eliminará la configuración del servidor VPN.

PASO 2 Para eliminar el servidor VPN y cerrar la ventana, haga clic en **Sí**.

PASO 3 Para guardar sus cambios y cerrar la ventana, haga clic en **Aceptar**.

Cuentas de usuario

Para crear una cuenta de usuario y definir una contraseña para los usuarios que soliciten una conexión por medio del túnel VPN, haga clic en **Crear**, y utilice la ventana **Agregar una cuenta**. Consulte **Agregar una cuenta, página 269**.

Para eliminar una cuenta de usuario, seleccione la cuenta y haga clic en **Eliminar**.

Acceso a la red

Para activar el acceso a Internet a través del túnel VPN para un sitio remoto, marque la casilla **Activar el acceso a Internet en sitio remoto**.

Si se activa el acceso a Internet a través del túnel VPN, se desactiva la División de arquitectura de túneles.

Para activar la división de arquitectura de túneles e identificar las redes protegidas por cifrado, siga estos pasos:

PASO 1 Marque la casilla de verificación **Activar división de arquitectura de túneles**.

Sólo el tráfico destinado a la subred protegida se cifra y se envía por medio del túnel VPN hasta la red inicial. Todo el demás tráfico se envía a las subredes de destino, pero no se cifra, y no está protegido po un túnel VPN.

PASO 2 Haga clic en **Crear** y utilice la ventana **Agregar una red** (consulte **Agregar una red, página 268**).

Para eliminar una subred protegida, siga estos pasos:

PASO 1 Seleccione la red y la máscara.

PASO 2 Haga clic en **Eliminar**.

Perfil VPN

En la ficha Perfil VPN, se puede exportar un archivo de configuración de perfil (PCF) que sus usuarios de VPN pueden importar en el cliente EZVPN de Cisco para crear una nueva conexión.

Para poder hacerlo, el UC500 debe tener una dirección IP de WAN estática.

Para exportar un archivo PCF, haga clic en **Exportar perfil VPN**. La opción Exportar perfil VPN se desactiva si no se ha terminado de configurar el servidor VPN. Guarde el archivo .pcf en su máquina local y distribúyalo a sus usuarios VPN.

Instrucciones para importar archivos VPN

Los usuarios de VPN deben seguir estos pasos para importar el archivo PCF al cliente de EZVPN de Cisco.

PASO 1 Si es necesario, descargue e instale el cliente de EZVPN desde Cisco.com en www.cisco.com/go/vpnclient.

PASO 2 Inicie el cliente de EZVPN de Cisco.

PASO 3 En el cliente de VPN, haga clic en el icono Importar o selecciones **Conexión** > **Importar** en la barra de menú y navegue hasta la ubicación del archivo PCF en la máquina local. Aparecerá el perfil como una nueva entrada de conexión.

PASO 4 Para utilizar el perfil, haga doble clic en la nueva entrada de conexiones y especifique su nombre de usuario y contraseña para su cuenta de VPN.

VPN remota

Para configurar la configuración VPN remota, seleccione **Configurar** > **Seguridad** > **VPN Remota** en la barra de funciones.

NOTA En los router seguros modelso SR520-T1, la VPN remota es una función bajo licencia. Para utilizar legalmente esta función de seguridad, se debe comprar la Licencia de función de seguridad FL-SR520-T1-SEC para el SR520-T1. Comuníquese con su distribuidor Cisco para comprar esta licencia.

Para activar los servicios del cliente remoto VPN en un router seguro SR500, siga estos pasos:

PASO 1 Comience seleccionando el dispositivo para configurar de la lista **Nombre de host**.

PASO 2 Para activar los servicios de voz, marque la casilla **Activar servicios de voz en conexión remota**.

PASO 3 En el campo **Dirección IP PBX**, especifique la dirección IP CME (Cisco Unified Communications Manager Express). Para el UC500, el valor por defecto es 10.1.1.1.

PASO 4 En el campo **Servidor VPN** , especifique la dirección IP o el nombre de host del servidor VPN o concentrador.

PASO 5 *Opcional*: En el campo **Especifique la nueva clave previamente compartida**, especifique una clave previamente compartida para autenticar los túneles cifrados.

La clave previamente compartida debe tener al menos 8 caracteres alfanuméricos y puede contener hasta 127 caracteres. No se admiten espacios ni signos de interrogación (?). Si se configura una clave previamente compartida en el dispositivo remoto VPN, ésta debe coincidir con la clave previamente compartida de un servidor VPN.

PASO 6 En el campo **Repita clave previamente compartida**, especifique la clave previamente compartida nuevamente.

PASO 7 Para guardar sus cambios y cerrar la ventana, haga clic en **Aceptar**.

Para eliminar la autorización del dispositivo remoto para que reciba políticas IPsec, siga estos pasos:

PASO 1 Haga clic en **Eliminar**.

Aparecerá una ventana, advirtiéndole que si continúa, eliminará la configuración remota VPN.

PASO 2 Para guardar sus cambios y cerrar la ventana, haga clic en **Aceptar**.

Establecer un túnel VPN (Instrucciones de conexión de cliente del usuario final)

Estas instrucciones describen cómo un usuario final conectado a un proveedor de servicio utilizando un router Cisco SR520 puede establecer un túnel VPN hacia una red central. Estas instrucciones se entregan para la conveniencia de un administrador de sistemas.

Para estableceer un túnel VPN entre un usuario remoto y una red central, siga estos pasos:

PASO 1 Abra una ventana de su navegador web, como Internet Explorer.

PASO 2 Especifique la dirección IP del servidor VPN en el campo **Dirección** del navegador. Aparecerá la ventana Herramienta de activación del túnel VPN entregando la opción de conectarse a una red central utilizando una VPN o por medio de Internet.

PASO 3 Para conectarse a la red central, haga clic en **Conectar ahora.** Aparecerá la ventana Autenticación para activación del túnel VPN .

PASO 4 Haga clic en **Continuar**. Queda establecido el túnel VPN.

Agregar una red

Esta ventana aparece cuando se hace clic en **Crear** en la ficha Acceso a la red en la ventana del Servidor VPN y se activa División de arquitectura de túneles.

Utilice esta ventana para agregar las subredes para las que los paquetes se dividen en túneles desde los clientes de VPN o de VPN SSL. Sólo el tráfico destinado a etas subreded se envía a través del túnel VPN o VPN SSL. Todo el tráfico restante desde las conexiones del cliente se envía sin cifrar. Para obtener más información, consulte **Acceso a Internet — División de túneles, página 262**.

Para agregar una red, siga estos pasos:

PASO 1 En el campo **Red**, especifique la dirección IP de la red.

PASO 2 En el campo **Máscara de Subred** , seleccione la máscara de la subred.

PASO 3 Siga agregando subredes para las que desee permitir el acceso a la VPN o VPN SSL.

PASO 4 Para cerrar la ventana, haga clic en **Aceptar**.

Agregar una cuenta

Esta ventana aparece cuando hace clic en **Crear** en la ficha Cuentas de usuarios en la ventana Servidor VPN.

Utilice esta ventana para agregar detalles de autenticación de usuarios a la base de datos local.

Para agregar una cuenta, siga estos pasos:

PASO 1 En el campo **Nombre de usuario**, especifique el nombre de usuario. El nombre de usuario puede contener hasta 64 caracteres alfanuméricos. No se admiten los siguientes caracteres: (espacio), +, #, %, /, \, ?, ; ,<, >, {, }, |, ^, ~, [,], `, ni ".

La cuenta del administrador se activa automáticamente como usuario de la VPN.

No puede eliminarse la cuenta de usuario de VPN por defecto.

PASO 2 Especifique la contraseñaa en el campo **Contraseña** y nuevamente en el campo **Confirmar contraseña**. La contraseña puede contener hasta 25 caracteres alfanuméricos. El largo mínimo de una contraseña es de 6 caracteres. No se admiten los siguientes caracteres: (espacio), +, ?, /, \, <, >, #, %, {, }, |, ^, ~, [,], `, ni ".

PASO 3 Para cerrar la ventana, haga clic en **Aceptar**.

Firewall y DMZ

Para configurar la configuración del Firewall y de DMZ, seleccione **Configurar** > **Seguridad** > **Firewall y DMZ** en la barra de funciones.

PRECAUCIÓN Cisco no recomienda que se configure el Firewall y la DMZ en una conexión WAN remota. Si se interrumpe la conexión a la WAN, fallará la operación y el sistema se volverá inutilizable.

Visión general

Se puede aumentar la seguridad de su red configurando un firewall y una zona desmilitarizada (DMZ) para proteger su LAN.

- Si se está configurando un UC520, se está utilizando un Firewall CBAC.
- Si se está configurando un SR520, se está utilizando un Firewall basado en zonas.

La política del firewall CBAC se define aplicando una configuración de Lista de control de acceso (ACL) estática en las interfaces de los routers para definir los tipos de tráfico que se permiten a través de una interfaz.

El firewall de políticas basadas en zonas cambia el modelo de inspección de estado de IOS de Cisco a
un modelo de configuración basado en zoneas donde las interfaces del router se asignan a zonas de seguridad, y la política de inspección del firewall se aplica al tráfico que se desplaza entra las zonas. (Vea “la Diferencia conceptual entre Cisco IOS Classic yaquellos basados en zonas", disponible en Cisco.com, para obtener mayor información).

Gestione la seguridad de su red realizando las siguientes tareas:

- Configure un firewall para filtrar los paquetes que llegan al router, de acuerdo con el nivel de seguridad que seleccione. Si un paquete cumple con los criterios, se le permitirá pasar a través de la interfaz o de la zona. Si un paquete no cumple con los criterios especificados por los parámetros de seguridad, éste se rechaza.
- Cree una DMZ en la que se ubiquen los servidores de acceso público, para que estén en una red separada y aislada. Ello entrega un nivel de seguridad adicional para su red interna. La DMZ puede utilizarse para el acceso público hacia Internet y para el acceso desde Internet hacia sus servidores que tengan acceso desde ella. Para crear una DMZ, primero se debe crear un firewall.

Procedimientos

Seleccione un dispositivo en el que desee activar un firewall (y opcionalmente una zona desmilitarizada) de la lista de **Nombre de host**.

Esta ventana tiene dos fichas:

- **Firewall, página 271**
- **DMZ, página 272**

En esta ventana también se puede hacer clic en **Servicio NAT** para abrir la ventana NAT para configurar las traducciones de direcciones de red. Consulte **Ventana NAT (Direcciones IP asignadas a través de DHCP), página 257**.

Firewall

Se sigue el mismo procedimiento para crear o modificar un firewall. Siga estos pasos:

PASO 1 Seleccione una interfaz externa de la lista **Interfaz/Zona externa (no fiable)**, o marque una interfaz interna en la lista **Interfaz/Zona interna (fiable)**. Las interfaces externas se conectan a su WAN o a Internet. Las interfaces internas se conectan a su LAN. Estas pautas se aplican:

- Si selecciona una interfaz externa, la **Interfaz/Zona interna (fiable)** se muestra de color gris.
- Se puede seleccionar múltiples interfaces.
- No seleccione la interfaz a través de la que ha accedido al Configuration Assistant de Cisco como la interfaz externa (no fiable).
- No se puede iniciar Configuration Assistant de Cisco a través del firewall desde la interfaz externa (no fiable).
- Si selecciona una interfaz externa que ya esté seleccionada como interfaz interna o interfaz DMZ, aparecerá un mensaje de advertencia.
- Si selecciona una interfaz interna que ya está seleccionada como interfaz DMZ, aparecerá un mensaje de advertencia.

PASO 2 Desplace el indicador de **Nivel de seguridad** hasta el nivel que desee. El indicador de Nivel de seguridad está activo cuando se selecciona una interfaz. El área de **Descripción** indica las normas de filtrado para cada uno de estos niveles de seguridad:

- **Alta** impide el uso de mensajería instantánea y aplicaciones punto a punto en la red. El firewall monitorea el tráfico HTTP y de correo electrónico y rechaza el tráfico que no cumple con el protocolo de seguridad. Devuelve otro tráfico de TCP (Protocolo de Control de Transmisión) y de UDP (Protocolo de Datagrama de Usuario) para sesiones iniciadas dentro del firewall.
- **Media** monitorea el uso de mensajería instantánea y aplicaciones punto a punto en la red, así como el tráfico HTTP y de correo electrónico. El firewall devuelve otro tráfico TCP y UDP para las sesiones iniciadas dentro del firewall.

- **Baja** no monitorea el tráfico de las aplicaciones. El firewall devuelve otro tráfico TCP y UDP para las sesiones iniciadas dentro del firewall.

PASO 3 En el campo **DNS Primario** , especifique la dirección IP del servidor DNS (Servicio de Nombre de Dominio) primario. Estas restricciones se aplican:

- Si se configuró el DNS a través de otros medios, no pueden configurarse las direcciones IP de DNS. Para modificar la configuración de DNS, utilice la ficha **Configuración de dispositivos** en la ventana **Configurar** > **Propiedades del dispositivo** > **Direcciones IP**.
- Si ya hay una DNS configurada en el dispositivo, aparece la dirección IP del DNS y no se puede especificar una dirección IP de DNS.
- Si el indicador de Nivel de seguridad está ubicado en medio o alto y no se ha configurado DNS en el dispositivo, se necesita una dirección IP primaria de DNS.

PASO 4 *Opcional*. En el campo **DNS secundario** , especifique la dirección IP del servidor DNS (Servicio de Nombre de Dominio) secundario.

DMZ

Para crear una DMZ, siga estos pasos:

PASO 1 En el menú **Interfaz DMZ** , seleccione una interfaz.

Si la interfaz que seleccionó es una interfaz externa o una interfaz interna que también se identifica como la interfaz para el firewall, aparecerá un diálogo de advertencia.

PASO 2 Haga clic en **Crear** y utilice la ventana Crear Servicio DMZ. Consulte **Crear Servicio DMZ, página 273**.

PASO 3 Para guardar sus cambios y cerrar la ventana, haga clic en **Aceptar**.

Para eliminar una DMZ, siga estos pasos:

PASO 1 Seleccione la dirección IP.

PASO 2 Haga clic en **Eliminar**. Aparecerá una ventana de confirmación.

PASO 3 Para cerrar la ventana, haga clic en **Sí**.

PASO 4 Para guardar sus cambios y cerrar la ventana, haga clic en **Aceptar** en la ventana Firewall y DMZ.

Crear Servicio DMZ

Esta ventana aparece cuando se hace clic en **Crear** en la ficha DMZ de la ventana Firewall y DMZ.

Utilice este diálogo para agregar una zona desmilitarizada (DMZ) a una interfaz. Primero debe configurar un firewall.

Siga estos pasos:

PASO 1 Para determinar hacia dónde se direccionarÃ¡ el tráfico para el servicio TCP o UDP especificado, indique una dirección IP en el campo **Dirección IP**. Si se activa NAT (Traducción de Direcciones de Red), especifique la dirección traducida por NAT, también conocida como la dirección global interna.

PASO 2 De la lista **Tipo de servidor**, seleccione el tipo de servidor admitido. Los tipos de servidores admitidos son **FTP**, **servidor Web, servidor Web seguro**, **servidor de correo**, **SSH** y **SFTP**.

PASO 3 Para cerrar la ventana, haga clic en **Aceptar**.

Firewall - Editar ACL

La ventana de Firewall - Editar ACL se muestra cuando:

- Se activa el firewall en el UC500.
- Se configuraron ACE (entradas de control de acceso) personalizadas fuera de banda utilizando la interfaz de línea de comandos de IOS.
- Configuration Assistant detecta la configuración fuera de banda cuando se intenta aplicar la configuración de voz.

Use los controles **Desplazar hacia arriba** y **Desplazar hacia abajo** de la ventana para volver a ordenar las entradas de la lista de control de acceso (ACL) según sea necesario, luego, haga clic en **Aceptar**.

Auditoría de seguridad

Para configurar una auditoría de seguridad, seleccione **Configurar** > **Seguridad** > **Auditoría de seguridad** en la barra de funciones.

Visión general

Se puede probar las políticas de seguridad y activar procedimientos de seguridad para garantizar servicios de red seguros en su red. Al auditar la configuración de su router, puede probar la funcionalidad de seguridad crítica de la configuración de su router para determinar si existen potenciales problemas de seguridad. Puede seleccionar aceptar o rechazar la configuración de seguridad recomendada.

Se verifican las siguientes condiciones. Puede cambiar la configuración según sea necesario para ajustar la seguridad de su red:

- Desactive el servicio finger
- Desactivar el servicio PAD
- Desactivar el servicio de pequeños servidores TCP
- Desactivar el servicio de pequeños servidores UDP
- Desactivar el servicio del servidor IP BOOTP
- Desactivar el servicio de identificación IP
- Desactivar la ruta de origen IP
- Activar el servicio de cifrado de contraseña
- Activar los paquetes "keep-alive" de TCP para sesiones Telnet entrantes
- Activar los paquetes "keep-alive" de TCP para sesiones Telnet salientes
- Activar números de secuencias y marcas horarias en las depuraciones
- Activar CEF (Cisco Express Forwarding) IP
- Desactivar Gratitous ARP de IP
- Definir la longitud mínima de la contraseña a menos de seis caracteres
- Definir la proporción de fallos de autenticación a menos de tres intentos
- Configure el tiempo de espera de sincronización TCP
- Activar registro

- Desactivar SNMP
- Definir la ubicación de un programador
- Desactivar los redireccionamientos IP
- Desactivar ARP Proxy IP
- Desactivar difusión dirigida IP
- Desactivar el servicio MOP (Protocolo de Operaciones de Mantenimiento)
- Desactivar las IP de destino inalcanzable
- Desactivar la respuesta de máscara IP
- Desactivar las IP de destino inalcanzable en una interfaz nula
- Activar RPF unidifusión en las interfaces externas
- Activar AAA

Procedimientos

Para ejecutar una auditoría de seguridad en un dispositivo, siga estos pasos:

PASO 1 Seleccione **Auditoría de seguridad** en la lista **Seguridad** para visualizar el botón de inicio de la Auditoría de seguridad.

PASO 2 De la lista **Nombre de host**, seleccione el dispositivo que se va a auditar.

PASO 3 Para mostrar una lista de la configuración de auditoría de seguridad y las acciones recomendadas, haga clic en **Auditoría de seguridad**. Aparece la ventana Reporte de auditoría de seguridad.

PASO 4 Use esta ventana para seleccionar cuáles acciones se realizarán para asegurar su red.

La tabla muestra cuáles parámetros de seguridad se configuran con los valores recomendados y cuáles no. Aquellos que no estén configurados con los valores recomendados representan un potencial problema de seguridad.

Para modificar la configuración de seguridad de un dispositivo, siga estos pasos:

PASO 1 Seleccione un dispositivo para auditar de la lista **Nombre de host**.

PASO 2 Para realizar la configuración de seguridad recomendada para los parámetros que no están definidos con los valores recomendados, haga clic en el botón de radio **Arreglar problemas de seguridad**. Para configurar la función de seguridad con los valores por defecto, haga clic en el botón **Deshacer configuración de seguridad**.

PASO 3 Para configurar las funciones de seguridad con los valores recomendados, marque las casillas de verificación de la columna **Definir** al lado de la configuración de seguridad que no aprobó la auditoría de seguridad.

PASO 4 Para configurar las funciones de seguridad con los valores por defecto, en la columna **Deshacer** al lado de los la configuración que aprobó la auditoría, marque las casillas de verificación. Para seleccionar todas las casillas, marque **Seleccionar todo**.

PASO 5 Haga clic en **Aceptar** para que los cambios surjan efecto y cerrar la ventana.

Configuración de seguridad de red (Switches CE520)

Si se encuentran presentes uno o varios switches Catalyst Express CE520 en el sitio del cliente, seleccione un nivel de seguridad para estos switches seleccionando **Configurar** > **Seguridad** > **Configuración de seguridad de red**.

Visión general

Debe configurar todos los switches Catalyst Express de su red con el mismo nivel de seguridad: inferior, medio o superior. Los niveles se definen de la siguiente forma:

- **Inferior**. Control de transmisiones intensas y control sobre el número de usuarios que puede acceder a un puerto
- **Medio**. Configuración baja, más una tabla para autorizar las direcciones MAC que pueden acceder a un puerto.
- **Superior**. Configuración baja más un servidor RADIUS identificado para la autorización de los dispositivos host que desean acceso.

Procedimientos

Aparece la ventana Configuración de seguridad de red cuando:

- La ventana Notificación de eventos muestra un conflicto en la configuración de seguridad de la red y usted hace clic en **Resolver**.
- Se selecciona Configurar **Configurar** > **Seguridad** > **Configuración de seguridad de red** en la barra de funciones.

Los contenidos de la ventana dependen de si usted configuró el nivel de seguridad de acceso de host en Inferior, Medio o Superior.

La ventana Notificación de eventos lo dirige a esta ventana por cualquiera de estas razones:

- Sus switches Catalyst Express no están configurados al mismo nivel de seguridad. Para resolver el conflicto, configure el nivel de seguridad en Inferior, Medio o Superior y haga clic en Aceptar.
- Una tabla de autenticación MAC contiene una dirección MAC que necesita su aprobación. Para realizar esta tarea, vea Nivel de host: Medio.
- La configuración de servidor RADIUS para sus switches Catalyst Express no es idéntica. Para realizar el conflicto, vea Nivel de host: Superior.

Nivel del host: Inferior

En el nivel Inferior, Network Assistant utiliza estas funciones de seguridad:

- Activar control de transmisiones intensas para todos los switches Catalyst Express en la comunidad.

  El control de transmisiones intensas evita que los paquetes de transmisión inunden la subred y degraden el rendimiento de la red. Una grave transmisión intensa puede bloquear todo el tráfico de la red.

- Activar puerto de seguridad para todos los switches Catalyst Express en la comunidad.

  El control de seguridad de puerto limita el número de direcciones MAC que pueden tener acceso a un puerto al mismo tiempo. El número máximo de direcciones MAC depende del perfil de Smartports que está configurado en el puerto. Esta tabla muestra cómo varían los máximos valores por perfil de Smartports.

Perfil de Smartports	Número máximo de direcciones MAC
escritorio	1

Perfil de Smartports	Número máximo de direcciones MAC
ipphone	3 si está configurada una VLANd de voz; de lo contrario, 2
punto de acceso	30
switch	Sin límite
Router	Sin límite
servidor	1
invitado	30
diagnóstico	Sin límite
otro	Sin límite

Para saber más sobre la función de Smartports, consulte **Smartports, página 162**.

Nivel del host: Medio

El nivel Medio agrega una función de seguridad llamada autenticación MAC. Esto significa que cuando un escritorio, servidor, impresora, teléfono IP, punto de acceso, switch o router se conecta a la comunidad a través de un puerto de switch Catalyst Express, su dirección MAC debe estar explícitamete agregada a la tabla de autenticación MAC antes de permitirle el acceso a la comunidad.

Usted agrega una dirección MAC a la tabla de autenticación MAC cuando:

- Usted conecta un dispositivo a un puerto en un switch Catalyst Express.
- Para aprobar la dirección MAC, usted selecciona sí en su celda Aprobada.
- Haga clic en **Agregar una dirección MAC** y utilice la ventana Agregar una dirección MAC. Consulte **Agregar una dirección MAC, página 279**.

Una direcciÃ³n MAC siempre estÃ¡ aprobada cuando se agrega.

Para cambiar la aprobación de una o más direcciones MAC, selecciónelas, haga clic en **Modificar** y use la ventana Modificar una dirección MAC. También puede cambiar la aprobación de una dirección MAC única al editar su celda Aprobada. Consulte **Modificar una dirección MAC, página 279**.

Para eliminar una o más direcciones MAC, selecciónelas y haga clic en **Eliminar**.

Las tablas de autenticación MAC en los switches Catalyst Express en su red deben ser idénticas. Si no lo son, se le solicita que resuelva el conflicto. Puede solicitar a Configuration Assistant que combine o borre las tablas.

Nivel del host: Superior

El nivel Superior configura 802.1x en switches Catalyst Express. 802.1x es un protocolo de autenticación que requiere que los host proporcionen sus nombres de usuario y contraseñas para acceder a la red. Se reenvían a un servidor RADIUS, donde se almacenan los nombres de usuario y contraseñas aprobados. Usted configura el servidor RADIUS en esta ventana.

NOTA La autenticación de 802.1x se aplica sólo a solicitudes de acceso desde escritorios.

Cuando usted utiliza el nivel Superior, ya no es necesaria la autenticación MAC, por ello, se desactiva.

Para configurar la autenticación 802.1x:

PASO 1 Especifique la dirección IP del servidor RADIUS.

PASO 2 Introduzca la clave RADIUS que los switches Catalyst Express usaá¡n para comunicarse con el servidor RADIUS.

PASO 3 Introduzca un puerto UDP desde 0 a 65535 para autorización de RADIUS. Si utiliza Cisco Secure ACS versión 4.0 o posterior, 1645 es el puerto UDP por defecto. Para versiones anteriores, es 1812.

Agregar una dirección MAC

Esta ventana aparece cuando usted configura la ventana Configuración de seguridad de red en el nivel de seguridad Medio y hace clic en **Agregar una dirección MAC aprobada previamente**.

Introduzca una dirección MAC en el campo Dirección MAC y haga clic en **Aceptar**. La dirección MAC aparecerá en la ventana Configuración de seguridad de red con un estado de aprobación de sí.

Modificar una dirección MAC

Esta ventana aparece cuando usted selecciona una o más direcciones MAC en la ventana Configuración de seguridad de red y hace clic en **Modificar**.

Si seleccionó una dirección MAC única, ella aparece en la ventana; si seleccionó más de una, verá Dirección MAC: Múltiple.

En la lista Aprobar, seleccione sí o no y haga clic en **Aceptar**. El estado de las direcciones MAC seleccionadas cambia en consecuencia.

VPN SSL

Para acceder a la configuración de la VPN SSL, seleccione **Configurar** > **Seguridad** > **VPN SSL**. Puede configurarse la VPN SSL en los routers seguros Cisco de la serie Cisco SR500.

Para activar y configurar la VPN SSL, el router debe tener una dirección IP estática.

NOTA Para el router seguro modelo SR520-T1, la VPN SSL es una función bajo licencia. Para utilizar legalmente esta función de seguridad, se debe comprar la Licencia de función de seguridad FL-SR520-T1-SEC para el SR520-T1. Comuníquese con su distribuidor Cisco para comprar esta licencia.

NOTA VPN SSL para el Dispositivo de seguridad de la serie SA500 de Cisco no se configura a través de CCA. Para configurar VPN SSL en este dispositivo, use la Utilidad de Configuración de Dispositivo de seguridad para el SA500.

PRECAUCIÓN Cisco no recomiendas que se configure VPN SSL en una conexión WAN remota. Si se interrumpe la conexión a la WAN, fallará la operación y el sistema se volverá inutilizable.

Visión general

La VPN (Red privada virtual) sobre SSL (Capa de conexión segura) entrega conectividad de acceso remoto desde casi cualquier ubicación con Internet utilizando un navegador web y su cifrado SSL nativo.

El principal perfil de SSL es entregar seguridad para el tráfico web. La seguridad incluye confidencialidad, integridad de mensajes y autenticación. SSL alcanza estos elementos de seguridad por medio de la utilización de criptografía, firmas y certificados digitales. Aunque la accesibilidad de la aplicación es limitada en

relación con las VPN de IPSec, las VPN basadas en SSL permiten el acceso a un conjunto cada vez mayor de aplicaciones de software comunes, servicios activados en la web, como acceso a archivos, correo electrónico y aplicaciones basadas en TCP (por medio de un cliente descargable).

Funciones básicas

La configuración de VPN SSL realizada por medio de CCA activa la configuración por defecto de mejores prácticas cuando sea posible.

Utilizando un navegador web con SSL activado (Internet Explorer, Netscape, o equivalentes), el usuario puede establecer una conexión con el gateway de VPN SSL. La solicitud inicial del usuario al gateway de la VPN SSl se responderá con una página HTML de inicio de sesión del usuario. El nombre de usuario y contraseña se envían al gateay para su autenticación con un servidor RADIUS (Cisco ACS) y sólo se inicia una sesión si la autenticación es exitosa.

Si se establece una sesión, se mantiene enviando un cookie de sesión al navegador del usuario. Esta cookie debe quedar incorporada a todas las posteriores solicitudes HTTP del usuario para su autenticación en el gateway de la VPN SSL. Si la cookie está ausente o es incorrecta, se cae la sesión y el usuario ya no podrá acceder a la red corporativa. Normalmente, la sesión permanece activa hasta que el usuario la cierre, se acabe el tiempo o la sesion se elimine del gateway de la VPN SSL.

La configuración básica de la VPN SSL entrega un modo sin clientes, con acceso seguro a recursos y contenidos web privados. Este modo es útil para entregar acceso a contenidos en un navegador web, como acceso a Internet, bases de datos y herramientas en línea que utilcen una interfaz web.

Cuando se configura SSL básica, una vez que el usuario se autentica y se inicia la sesión, aparece una página del portal de la VPN SSL y la barra de herramientas se agrega al navegador web del usuario. En esta página, el usuario puede acceder a todos los sitios HTTP disponibles, a su correo electrónico web y navegar por los servidores de archivos CIFS.

NOTA Si está activado un bloqueador de ventanas emergentes, es posible que la pequeña ventana de la barra de herramientas de la VPN SSL no aparezca.

Funciones avanzadas

Las opciones avanzadas de la VPN SSL entregan un modo de cliente liviano de SSL, y un modo de cliente de túnel completo.

- **Modo de cliente liviano (reenvío de puertos).** El modo de cliente liviano extiende la capacidad de las funciones criptográficas del navegador web para activar el acceso remoto a las aplicaciones basadas en TCP con

puertos estáticos, tales como POP3 (Protocolo de Oficina de Correos versión 3), SMTP (Protocolo Simple de Transferencia de Correo), IMAP (Protocolo de acceso a mensajes a través de internet), Telnet y SSH (Secure Shell).

En el modo de cliente liviano, el usuario de la VPN descarga un subprograma Java haciendo clic en el enlace que se entraga en la página del portal. El subprograma Java actúa como un proxy TCP en la máquina del cliente para los servicios configurados por el administrador del gateway de seguridad. La descarga en modo cliente liviano supone que el usuario que descarga el subprograma tiene privilegios administrativos.

- **Modo túnel completo**. El modo de cliente de túnel completo ofrece un vasto soporte de aplicaciones a través de su cliente descargado dinámicamente Cisco Anyconnect o del SVC (Cliente de la VPN SSL). El modo de cliente de túnel completo entrega un cliente de túnel de la VPN SSL que es liviano, se configura centralmente y al que es fácil dar soporte y que entrega acceso a las capas de la red para casi cualquier aplicación.

  En el modo de cliente de túnel completo, se utiliza un túnel sobre SSL para mover datos hacia y desde las redes internas de la capa de red (IP). Cuando el usuario inicia sesión en el portal de la VPN SSL, el cliente de la VPN SSL se descarga e instala en forma automática en la PC del usuario y se establece la conexión con el túnel. Una vez que se establece la conexión, el usuario tiene pleno acceso VPN a la red corporativa. También es posible utilizar el modo de túnel completo para tener soporte de voz.

  Cuando se activa el modo de Túnel completo, debe instalarse el cliente Anyconnect de la VPN la SSL para que funcione la VPN.

  NOTA El usuario de la VPN SSL debe tener derechos administrativos para instalar aplicaciones en su PC para que funcione la descarga e instalación automática del cliente de la VPN SSL.

  Es necesario iniciar sesión en Cisco.com para descarga el cliente. En la ficha Avanzadas se entrega un enlace a esta descarga de software para este paquete.

- **División de la arquitectura de túneles**. Cuando se active división de túneles en una red remota, las comunicaciones del cliente con los dispositivos locales o de Internet con otras redes quedan cifradas. Los datos sólo se cifran cuando el usuario final está comunicándose con un subred protegida, típicamente, la red corporativa. Ello reduce el tiempo de procesamiento del dispositivo y mejora el rendimiento de la red.

PRECAUCIÓN: La división de túneles puede presentar, potencialmente, un riesgo a la seguridad cuando esté configurada. Debido a que los clientes de VPN SSL tienen acceso no seguro a la Internet, ellos pueden quedar expuestos a un ataque. Dicho ataque podría lograr acceso a la LAN corporativa por medio del túnel utilizando la identidad del cliente.

Procedimientos

Comience seleccionando un dispositivo para configurar de la lista **Nombre de host**.

Esta ventana tiene dos fichas:

- **Básicas**
- **Avanzadas**

Básicas

En la ficha Básicas, configure los parámetros de acuerdo a la siguiente tabla, luego haga clic en **Aceptar** para cerrar la ventana.

Configuración	Descripción
Certificado digital	Seleccione el certificado digital que se enviará al cliente para la autenticación SSL. Si no se encuentra un certificado digital, haga clic en **General certificado** para generar uno.
Dirección IP	Este campo de sólo lectura sólo muestra la dirección IP de la WAN estática configurada. Esta es la dirección IP que se utilizará para acceder al portal de la VPN. **NOTA** Para iniciar la VPN SSL desde el PC del cliente, utilice el formato https://*dirección IP* en el campo **Dirección** del navegador (utilice https en vez de http).

Configuración	Descripción
Sitios web de Intranet	Lista de sitios web de Intranet que aparecerá en la página del portal de la VPN SSL. Para agregar un sitio web de intranet: 1. Haga clic en **Agregar** para insertar una fila en la tabla. 2. Haga clic en el campo **Etiqueta** de la nueva fila y especifique una etiqueta descriptica con carácteres alfanuméricos. No se admiten los siguientes caracteres: +, #, %, /, \, ?, ; ,<, >, {, }, |, ^, ~, [,], `, ni ".  3. Haga clic en el campo **URL** y especifique la URL para el sitio web. No se admiten los siguientes caracteres: (espacio), +, ?, /, \, <, >, #, %, {, }, |, ^, ~, [, ], `, ni ". Para eliminar un sitio web de Intranet, seleccione el sitio de la llista y haga clic en **Eliminar**.

Configuración	Descripción
Cuentas de usuario	Lista de cuentas de usuarios para esta VPN SSL. La cuenta del administrador se activa automáticamente como usuario de la VPN. El número máximo de cuentas de usuario es de 10 para las plataformas UC520 y UC540, y de 20 para las plataformas UC560. **NOTA** El número máximo de conexiones de VPN simultáneas que permite CCA para las plataformas UC520 y UC540 es de 10. Para las plataformas UC560, se permiten hasta 20 conexiones de VPN simultáneas. Las conexiones de VPN que se utilicen para EZVPN, VPN SSL, Administrador de múltiples sitios, y para las VPN de teléfonos SPA525G se incluyen en este total. Para agregar una cuenta de usuario y establecer una contraseña para los usuarios que necesitan una conexión por medio de un túnel de VPN: 1. Haga clic en **Agregar** para insertar una fila en la tabla. 2. Haga clic en el campo **Nombre de usuario** de la nueva fila y especifique la ID del usuario para la nueva cuenta. 3. Haga clic en el campo **Contraseña** y especifique la contraseña de la cuenta del usuario. No se admiten los siguientes caracteres: (espacio), +, ?, /, \, <, >, #, %, {, }, |, ^, ~, [,], `, ni ". Para eliminar una cuenta de usuario, seleccione la cuenta de la lista y haga clic en **Eliminar**.

Avanzadas

En la ficha Avanzadas, active y configure los parámetros avanzados de la VPN SSL de acuerdo con la siguiente tabla. Cuando termine, haga clic en **Aceptar** para cerrar la ventana.

Configuración	Descripción	
Cliente liviano	Active o desactive el modo de Cliente liviano (reenvío de puertos) para la VPN SSL. Cuando no se marca Cliente liviano, se utiliza el modo sin cliente.	
	Configurar lista de reenvío de puertos	Cuando se activa Cliente liviano, haga clic en **Configurar reenvío de puertos** para activar el acceso remoto a las aplicaciones basadas en TCP, como correo electrónico, Telnet y SSH con puertos estáticos. Complete la configuración en la ventana Reenvío de puertos, según se describe en **Configurar lista de reenvío de puertos, página 289**.

Configuración	Descripción	
Túnel completo	Active o desactive el modo Túnel completo para la VPN SSL. El modo túnel completo entrega un cliente de túnel liviano para la VPN SSL que entrega acceso a la capa de red para casi cualquier aplicación. El cliente se descarga e instala en forma automática en el PC del usuario. Para el modo Túnel completo, debe instalarse el cliente de VPN SSL. El usuario de la VPN debe tener derechos administrativos para instalar aplicaciones en su PC para que funcione la descarga e instalación automática del cliente de la VPN SSL. Cuando se active el modo Túnel completo, especifique un intervalo de direcciones IP para que los clientes las usen cuando se conecten.	
	IP inicial	Especifique la primera dirección IP del intervalo.
	IP final	Especifique la última dirección IP del intervalo.

Configuración	Descripción	
Cliente de VPN SSL	Cuando se activa el cliente de Túnel completo, se activan las opciones **Instalar** y **Desinstalar**. **IMPORTANTE** Cuando se activa el modo Túnel completo, es necesaria la instalación del cliente de VPN SSL. Si no está instalado el cliente, se muestra un mensaje de error para los usuarios. La opción Instalar le permite instalar el software de cliente de VPN SSL (paquete de implementación Web de clientes Anyconnect de Cisco enlos router seguros SR520-T1, o el cliente de VPN SSL (SVC) en Routers seguros SR520 ADSL/Ethernet).	
	Instalar	Para instalar el software del cliente de VPN SSL, haga clic en **Instalar**, haga clic en **Examinar** para buscar la ubicación del archivo y luego, haga clic en **Aceptar**. CCA admite el paquete de implementación web actual para Windows. Cuando se hace clic en **Instalar**, se entrega un enlace hacia la ubicación de la descarga de este paquete. Para descargar este software, es necesario iniciar sesión en Cisco.com. Consulte **Instalar ventana del software del cliente de la VPN SSL, página 291** para obtener mayores instrucciones.
	Desinstalación	Para desinstalar el software del cliente de la VPN SSL, haga clic en **Desinstalar**.
	Mantenga el software del cliente instalado en la PC del usuario.	Marque **Mantener software del cliente instalado en la PC del usuario** para dejar el software del cliente en la PC del usuario, para que no tenga que descargarse e instalarse cada vez que el usuario se conecte a la VPN SSL. **SUGERENCIA** Desactive esta opción si se está utilizando la VPN SSL para un acceso remoto por terceros, ya que no es bueno dejar una copia del cliente es PC externos.

Configuración	Descripción	
División de la arquitectura de túneles	**Activar la división de la arquitectura de túneles**	Marque esta opción para activar la división de la arquitectura de túneles. Sólo el tráfico destinado a la subred protegida se cifra y se envía por medio del túnel VPN SSL hasta la red inicial. Todo el demás tráfico se envía a las subredes de destino, pero no se cifra, y no está protegido por un túnel VPN SSL. Haga clic en **Agregar** para especificar las subredes locales para el tráfico de VPN SSL. Consulte **Agregar una red, página 268** para ver una descripción de los campos de este diálogo. Para quitar una subred de la lista, destaque la entrada de la subred de la lista y haga clic en **Quitar**.

Configurar lista de reenvío de puertos

Aparece la ventana Reenvío de puertos cuando se hace clic en **Configurar lista de reenvío** de puertos en la ventana de la VPN SSL.

Visión general

Cuando se activa el reenvío de puertos, el archivo host del cliente de la VPN SSL se modifica para mapear la aplicación al número de puerto configurado en la lista de reenvío. Un objeto de la Lista de reenvío de puertos define los mapeos de los números de puertos en el cliente remoto a la dirección IP de la aplicación y al puerto detrás del gateway de la VPN SSL.

Procedimientos

Para agregar una entrada a la lista de Reenvío de puertos para cada mapeo de servidor y puertos, haga clic en **Aceptar**, configure los parámetros para cada entrada según se describe a continuación, y luego, haga clic en **Aceptar** para cerrar la ventana y guardar su configuración.

Configuración	Descripción
IP servidor	Especifique una dirección IP que utilice el servidor. Se trata de una dirección IP que no puede utilizarse, externamente, en Internet.
Puerto del servidor	Especifique el número del puerto de la aplicación para la que se configure el reenvío de puertos (entre 1 y 65535). El puerto de servicio debe ser un puerto estático.
Puerto del cliente	Especifique el número del puerto del cliente (entre 1 y 65535). El puerto debe ser un puerto estático.
Descripción	Agregue información sobre la entrada de reenvío de puertos (hasta 1024 carácteres). Esta información es obligatoria en los routers IOS de Cisco.

Para eliminar un mapeo de reenvío de puertos, siga estos pasos:

PASO 1 Seleccione una entrada en la ventana.

PASO 2 Haga clic en **Eliminar**.

PASO 3 Haga clic en **Aceptar** para guardar sus cambios y cerrar la ventana.

Agregar una cuenta de usuario

Esta ventana aparece cuando se hace clic en **Agregar** en la ficha Cuentas de usuario de la ventana VPN SSL.

Para agregar una cuenta de usuario, configure los parámetros según se indica a continuación, luego haga clic en **Aceptar** para guardar sus cambios y cerrar la ventana.

NOTA La cuenta del administrador se activa automáticamente como una cuenta de usuario de VPN SSL y no puede ser eliminada.

Configuración	Descripción
Nombre de usuario	El nombre de usuario puede contener hasta 64 caracteres alfanuméricos. No se admiten los siguientes caracteres: (espacio), +, #, %, /, \, ?, ; ,<, >, {, }, |, ^, ~, [,], `, ni ".
Contraseña	La contraseña puede contener hasta 25 caracteres alfanuméricos. El largo mínimo de una contraseña es de 6 caracteres. No se admiten los siguientes caracteres: (espacio), +, ?, /, \, <, >, #, %, {, }, |, ^, ~, [,], `, ni ".
Confirmar contraseña	Especifique de nuevo la contraseña para confirmarla.

Agregar sitios web de Intranet

Esta ventana aparece cuando hace clic en **Agregar** (Sitios web de Intranet) en la ventana de la VPN SSL.

Para agregar una URL, configure los parámetros según se indica a continuación, luego haga clic en **Aceptar** para guardar sus cambios y cerrar la ventana.

Configuración	Descripción
Etiqueta de URL	Especifique una descripción de la URL utilizando carácteres alfanuméricos. No se admiten los siguientes caracteres: +, #, %, /, \, ?, ; ,<, >, {, }, |, ^, ~, [,], `, ni ".
URL	Especifique la URL. No se admiten los siguientes caracteres: (espacio), +, ?, /, \, <, >, #, %, {, }, |, ^, ~, [,], `, ni ".

Instalar ventana del software del cliente de la VPN SSL

Esta ventana aparece cuando hace clic en **Instalar (Software de cliente de la VPN SSL)** en la ventana de la VPN SSL.

Use esta ventana para instalar el software del cliente de la VPN SSL en el dispositivo del cliente. También puede utilizar esta ventana para descargar la última versión del software del cliente de la VPN SSL. Para descargar el software del cliente de la VPN SSL, es necesario iniciar sesión en Cisco.com.

Para instalar el software del cliente de la VPN SSL en el dispositivo del cliente, siga estos pasos.

PASO 1 Si es necesario, descargue el archivo .pkg de implementación web Cisco Anyconnect o del Cliente de la VPN SSL en Cisco.com utilizando el enlace que se entrega. Los puntos de enlace al paquete de clientes de Microsoft Windows actualmente admitidos.

Si se instala el paquete de software 8.1.0 para el UC500 en su sistema, se debe usar la versión 2.5.1025 del paquete de software para Anyconnect de Microsoft (win-2.5.1025-k9.pkg). Las versión 2.3.0254 del cliente Anyconnect es incompatible con la versión de IOS de Cisco contenida en el paquete de software 8.1.0 para el UC500.

PASO 2 Haga clic en **Examinar** y navegue hasta la ubicación del paquete de software del Cliente de la VPN SSL o Anyconnect en su PC local.

PASO 3 Seleccione el archivo .pkg del Cliente de la VPN SSL.

PASO 4 Haga clic en **Aceptar** para instalar el paquete y volver a la ventana de la VPN SSL.

Sistema de prevención de intrusiones (IPS)

Para configurar IPS en los routers seguros de la serie SR500, seleccione **Configurar** > **Seguridad** > **IPS** de la barra de funciones.

NOTA Para el router seguro modelo SR520-T1, IPS es una función bajo licencia. Para utilizar legalmente esta función de seguridad, se debe comprar la Licencia de función de seguridad FL-SR520-T1-SEC para el SR520-T1. Comuníquese con su distribuidor Cisco para comprar esta licencia.

Visión general

Un sistema de prevención de intrusiones monitorea las actividades de la red y/o del sistema en búsqueda de conductas maliciosas o indeseadas y poder reaccionar, en tiempo real, para bloquear o evitgar aquellas actividades.

Un IPS basado en red opera en línea para monitorear todo el tráfico de la red en búsqueda de código o ataques maliciosos. Cuando se detecta un ataque, se rechazan los paquetes maliciosos, pero se permite que todo el resto del tráfico pase. A diferencia de los firewall tradicionales, un IPS toma decisiones de control de acceso basado en el contenido de las aplicaciones, en vez de en direcciones o puertos IP.

El sistema de prevención se intrusiones (IPS) IOS de Cisco es una función de inspección en línea y de profundos paquetes que efectivamente mitiga una amplia variedad de ataques a la red y admite las siguientes funciones:

- IPS puede configurarse para las interfaces internas y externas que se consideren vulnerables a los ataques.
- Una vez que se configuren las interfaces IPS, se debe obtener una clave pública e importar un paquete de firmas IPS (Archivo de definición de firmas, o SDF). Sólo se admiten actualizaciones de firma IPS para los archivos SDM-IPS.
- Puede importar actualizaciones de paquetes de firma después de la configuración inicial.
- Se entregan Alertas de IPS para notificar a los usuarios de ataques y alertas, niveles de riesgo y medidas tomadas.

NOTA No se admiten las funciones de editar firmas, tablero de seguridad IPS ni el monitoreo de seguridad.

Procedimientos

Consulte los siguientes temas para configurar las fuciones IPS:

- **Configuración IPS inicial, página 293**
- **Actualizaciones de firmas IPS, página 295**
- **Alertas IPS, página 296**
- **Eliminar Configuración IPS, página 296**

Configuración IPS inicial

La configuración IPS inicial exige que usted seleccione un dispositivo en el cual activar IPS y también interfaces para la exploración de paquetes, obtenga una clave pública, descargue un paquete de firmas e instale el archivo de definición de firmas del paquete en el router.

Para configurar IPS, siga estos pasos:

PASO 1 Seleccione un dispositivo en el que desee activar IPS de la lista **Nombre del host**.

PASO 2 Configure las interfaces.

Para configurar interfaces para IPS, seleccione una interfaz externa de la lista **Interfaz/Zona externa (no fiable)**, o marque una interfaz interna en la lista **Interfaz/Zona interna (fiable)**. Las interfaces disponibles detectadas en el router se indica en las columnas Interna y Externa de la tabla.

Los términos *externa* e *interna* se refieren a la dirección para la exploración de paquetes IPS en búsqueda de ataques en la interfaz (flujo de paquetes entrantes o salientes).

- Cuando se selecciona IPS para una interfaz de la columna **Externa** de la tabla, IPS sólo explora los paquetes salientes de esa interfaz.
- En forma similar, cuando se selecciona IPS para una interfaz de la columna **Interna** de la tabla, IPS sólo explora los paquetes entrantes de esa interfaz.
- Las mismas interfaces pueden configurarse tanto como interfaces internas como externas.

Se puede activar la exploración IPS del flujo de paquetes entrantes y/o salientes de una interfaz y no existe límite en el número de interfaces para las que puede activarse IPS.

PASO 3 Descarga de una clave pública

Una vez que se ha configurado las interfaces interna y externa, haga clic en el enlace entregado para descargar una clave pública de Cisco.com. Luego, copie y pegue la sección de la **cadena de la clave** en el área de texto que se entrega para la clave.

La clave pública es obligatoria y recibe el nombre de **realm-cisco.pub**.

PASO 4 Descargue e instale un paquete de firmas.

Necesitará entregar su inicio de sesión y contraseña de su cuenta de usuario de Cisco.com para la autenticación.

Para descargar e instalar un paquete de firmas IPS:

a. Haga clic en **Instalar SDF** para abrir el diálogo Descargar paquete de firma con un enlace para descargar un paquete de archivos de definición de firmas (SDF) para SDM-IPS.

b. Haga clic en el enlace de descarga para ir a Cisco.com y seleccione un paquete de firmas para SDM-IPS de Cisco IOS de lalista de paquetes de firmas para SDM-IPS.

   Sólo se admite utilizar los paquetes de SDM-IPS de la categoría Básica con el SR520. La categoría básica soporta archivos de firmas de hasta 128 MB de tamaño y está diseñado para routers con hasta 128 MB de memoria.

c. Naveque hasta la ubicación del archivo del paquete de firmas (formato .zip) en su PC local.

d. Haga clic en **Aceptar** o **Aplicar**.

Cuando se hace clic en **Aceptar** o en **Aplicar**, se envía la configuración al router. Todos los archivos de configuración relativos a IPS se encuentran en la siguiente ubicación: flash:/ips/

Una vez que se ha instalado el paquete de firmas, se activa el botón **Eliminar configuración IPS**, la ficha **Actualizaciones de firmas IPS** y la ficha **Alertas IPS**.

Actualizaciones de firmas IPS

Las actualizaciones de firmas IPS sólo están disponibles si IPS se configuró con éxito y se descargó un paquete de firmas.

Sólo se admiten actualizaciones de firma IPS para los archivos SDM-IPS. En la ficha Actualizaciones de firma IPS, se puede importar firmas nuevas y actualizadas para un paquete SDF seleccionado.

Para importar actualizaciones de firmas IPS, siga estos pasos:

PASO 1 En ventana IPS, haga clic en la ficha Actualizaciones de firmas IPS.

PASO 2 Haga clic en el enlace para ir a Cisco.com y seleccione un archivo del paquete .sdf de IPS-SDM que va a descargar.

PASO 3 Navegue hasta la ubicación del archivo del paquete SDF (formato .zip) en su PC local.

PASO 4 Haga clic en **Extraer firmas** para mostrar las firmas nuevas y actualizadas, así como también las firmas que se implementan en el router, pero que están desactivadas en este momento.

PASO 5 Haga clic en **Aceptar** para descargar al router las firmas que aparecen en la tabla y actualizar la versión del paquete SDF en el router.

Alertas IPS

La sección Alertas IPS muestra las alertas de detección de intrusiones y las medidas que se toman, junto con información sobre la alerta. Para cada alerta, se muestra la siguiente información:

- ID de la firma y descripción del ataque
- Nivel de riesgo
- Acciones del evento
- Direcciones IP de origen y destino del ataque
- Cantidad de hits y de paquetes rechazados

Haga clic en **Mostrar alertas** para ver la lista actual de alertas; haga clic en **Borrar alertas** para borrar la lista.

Eliminar Configuración IPS

Para eliminar la configuración IPS actual, haga clic en **Eliminar configuración IPS**, y luego, seleccione **Aceptar** o **Aplicar**.

Filtro de URL (serie SR500)

Para configurar el Filtro de URL en los routers seguros de la serie Cisco SR500, seleccione **Configurar** > **Seguridad** > **Filtro de URL**.

Debe activarse la configuración de ZBF (Firewall basado en zonas) antes de que se pueda activar el filtro de URL.

NOTA Para el router seguro modelo SR520-T1, Filtro de URL es una función bajo licencia. Para utilizar legalmente esta función de seguridad, se debe comprar la Licencia de función de seguridad FL-SR520-T1-SEC para el SR520-T1. Comuníquese con su distribuidor Cisco para comprar esta licencia.

Visión general

El filtro de URL permite controlar el acceso a los sitios web de Internet al permitir o negar el acceso a sitios web específicos basados en una lista de URL. Se pueden mantener una lista de URL local en el router.

CCA sólo admite listas en Blanco/Negro (Filtro de URL C3PL). Una lista de Blanco/Negro es una lista de URL que se crea manualmente y la mantiene el personal de seguridad de la red de una empresa. No existen URL por defecto, las definen los usuarios. CCA actualmente no admite el uso de servidores de terceros para el filtro de URL.

La lista de Blanco/Negro:

- Entrega una solución básica si se necesita eximir a unas pocas URL específicas.
- Permite que una empresa administre directamente las URL restringidas como parte de una política corporativa.
- Aprovecha los equipos de red existentes.

Procedimientos

PASO 1 Seleccione un dispositivo en el que desee administrar el filtro de URL de la lista de **nombres de host**.

PASO 2 configure las opciones del filtro y administre la lista de nombre de dominio que se van a filtrar:

a. Marque la casilla **Activar** para activar el filtro de URL.

   Cuando se desactiva el filtro URL, aún se puede agregar y eliminar URL de la lista de nombres de dominio, pero no se ejecuta el filtrado. Por defecto, el filtro URL está desactivado.

b. Seleccione si se debe denegar todos los dominios, excepto aquellos indicados, o permitirlos a todos, excepto los indicados.

   Para agregar una URL a la lista de nombres de dominio que se van a filtrar, haga clic en **Agregar**, luego, en la fila que acaba de agregar y especifique el nombre del dominio. Se aceptan noombres de dominion parctiales, siempre que puedan validarse (por ejemplo, cisco.com es válido).

La cantidad máxima de URL que permite la lista del filtro es 100.

c. Siga agregando y eliminando nombres de dominio según sea necesario.

PASO 3 Haga clic en **Aceptar** o **Aplicar**.

Una vez que haga clic en **Aceptar** o **Aplicar**, no puede modificar los nombres de la lista. Se debe eliminar y, luego, volver a agregar el nombre para poder cambiarlo.

También puede importar un archivo de texto con una lista de URL que se van a filtrar o exportar la lista actual de URL a un archivo de texto que pueda importarse a otro dispositivo o aplicación. Las siguientes pautas se aplican a la creación de archivos de listas de URL:

- La extensión del nombre del archivo debe ser .csv, o .txt.
- Las líneas que comienzan con "#" se consideran comentarios.
- No se admiten duplicados en la lista.
- Las URL se especifican una por línea, como se indica en el siguiente ejemplo:

```
#Nombre de dominio
www.cisco.com
www.yahoo.com
www.rediffmail.com
www.google.com
```

9

Configuración de región y sistema de telefonía

Esta sección cubre la configuración del sistema y de la región para Telefonía. Se cubren los siguientes temas:

- **Inicio del sistema de voz**
- **Configuración del sistema de voz**
- **Configuración regional para telefonía**

IMPORTANTE Debe estar activado el acceso a Telnet para poder configurar las funciones de voz.

Inicio del sistema de voz

La ventana de Inicio de voz aparece cuando se intenta abrir una ventana de configuración de voz antes de iniciar la configuración de voz en el nivel de sistema.

Si no está usando el Asistente de configuración de telefonía, se debe configurar esto antes de poder configurar las funciones de voz.

Si la plataforma UC500 que se está configurando está en modo por defecto de fábrica, recomendamos que use el Asistente de configuración de telefonía para configuirar estos parámetros y definir los enlaces troncales. Para obtener más información, consulte **Asistente de configuración de telefonía, página 98**.

Luego de haber aplicado esta configuración, el sistema ya no está en estado por defecto de fábrica, y no se puede usar el Asistente de configuración de telefonía hasta que se restablezca la configuración por defecto de fábrica en el UC500.

Haga clic en **Aceptar** cuando termine, o en **Cancelar**.

Campo	Descripción
Modo del sistema	Seleccione si se configura la gestión de llamadas para **PBX** o **Sistema de claves**. El valor por defecto es PBX. Cuando el **Mododel sistema** se configura como **Sistema de claves**, el sistema entra en modo híbrido, donde los enlaces SIP se tratan como si el sistema estuviera en modo PBX, y los enlaces locales (FXO, BRI, PRI) se tratan como líneas del sistema de claves. En este modo, los enclaces FXO y los enlaces T1/E1 CAS se configuran como líneas de enlace directo. A diferencia de versiones anteriores de CCA (1.x), no hay diferencia real entre el modo Sistema de claves y PBX.
Número de dígitos por anexo	Configure la longitud del anexo. El valor por defecto es 3.
Anexo de acceso a correo de voz	Anexo interno para acceder al sistema de correo de voz. El número de dígitos en el anexo debe coincidir con el **Número de dígitos por anexo** especificado.

Configuración del sistema de voz

Para acceder a esta configuración, seleccione **Configurar** > **Telefonía** > **Sistema** > **Configuración del sistema**.

En la ventana Sistema, se realiza la siguiente configuración:

- **Configuración de hardware**
- **Mensaje del sistema**
- **Configuración del tipo de sistema**

Haga clic en **Aceptar** o en **Aplicar** cuando haya finalizado de hacer cambios en esta configuración.

Configuración de hardware

La configuración del hardware del UC500 se detecta y se muestra en la sección Configuración del hardware. CCA limita los parámetros de configuración abiertos a modificación, de acuerdo con la configuración de hardware del router. Típicamente, estos parámetros son fijos.

Mensaje del sistema

En el campo Mensaje del sistema, especifique un mensaje que aparecerá en los teléfonos, por ejemplo, el nombre de la empresa. El mensaje puede tener hasta 31 caracteres.

Si el campo Mensaje del sistema se deja en blanco (sin texto alfanumérico) cuando se aplica la configuración, el mensaje no se actualiza y permanecerá el mensaje del sistema existente que se indica en los teléfonos.

Configuración del tipo de sistema

Sólo está disponible la configuración del tipo de sistema para la configuración inicial:

- Esta configuración también puede realizarse con el Asistente de configuración de telefonía o en la ventana Inicio de voz.
- Se debe restablecer el UC500 a los valores de fábrica por defecto para cambiar esta configuración.
- Después de aplicar esta configuración, los campos quedan de sólo lectura.

Configuración	Descripción
Tipo de sistema de voz	Seleccione un tipo de sistema de voz, ya sea **PBX** o **Sistema de claves**. Cuando se selecciona **Sistema de claves**, los enlaces SIP se tratan como líneas PBX y los enlaces locales (FXO, BRI, PRI) se tratan como líneas del sistema de claves. Los enclaces FXO y los enlaces T1/E1 CAS se configuran como líneas de enlace directo. No hay otras diferencias entre el modo Sistema de claves y PBX.

Configuración	Descripción
Número de dígitos por anexo	Especifique el número de dígitos para los anexos en el sitio del cliente. El valor por defecto es 3.

Configuración regional para telefonía

Para configurar la región para Telefónía, seleccione **Configurar** > **Telefonía** > **Sistema** >**Región** en la barra de funciones.

En esta ventana, se puede seleccionr el:

- País para los tonos de progreso de llamadas
- Idioma y regiones para teléfonos
- Idioma del correo de voz
- Formato que se usará para mostrar la fecha y hora en los teléfonos

La localización del sistema por defecto para el UC 500 es Inglés de Estados Unidos. Antes de realizar configuraciones de localizaciones que no sean de Estados Unidos en la ventana Región, se debe descargar el paquete de software y/o paquete de localización adecuados para el UC500 (que contienen los archivos para localizar los teléfonos y el correo de voz) e instalarlos en el UC500. Consulte **Instalación de software del UC500, página 556** y **Cómo localizar el UC500 (localizaciones diferentes a Inglés de EE.UU.), página 573**.

Se puede instalar hasta dos idiomas en el UC500, pero sólo uno puede estar activo. Si se han instalado dos idiomas, se puede cambiar cuál de ellos está activo en esta ventana. Para instalar idiomas adicionales, seleccione **Mantenimiento** > **Actualización de software** > **UC500**.

Definir configuraciones de región

En la ventana Región, se puede determinar la siguiente configurar local para telefonía. Cuando haya finalizado, haga clic en **Aceptar** o **Aplicar**.

Configuración	Descripción
Dispositivos	

Configuración	Descripción
Su nombre de host	Asegúrese que está seleccionado el nombre del host del UC500.
Tono de progreso de llamadas	
País	Seleccione el páis adecuado para definir tonos y cadencias para los teléfonos.
Teléfonos Las selecciones de idioma y regiones de teléfonos que se muestran aquí corresponden a los archivos de localización e idioma para teléfonos instalados en el UC500. Por defecto, es Inglés de Estados Unidos. Si no se instalan otros idiomas, no se indican otras opciones. Para instalar idiomas adicionales, seleccione **Mantenimiento** > **Actualización de software** > **UC500**. Consulte **Instalación de software del UC500, página 556**.	
Región de teléfonos	Seleccione la localización adecuada para esta instalación.
Idioma telefónico	Seleccione el idioma que aparecerá en los teléfonos.
Correo de voz	
Idioma del correo de voz	Idioma de los saludos del correo de voz que los usuarios escucharán. En un sistema por defecto de fábrica, sólo está disponible Inglés en el menú desplegable de Idima de correo de voz. Se debe descargar en instalar los paquetes de localización adecuados para el UC500 para localizar el sistema de correo de voz. Para instalar idiomas adicionales, seleccione **Mantenimiento** > **Actualización de software** > **UC500**. Consulte **Instalación de software del UC500, página 556** para obtener mayor información acerca de la localización del sistema de correo de voz instalando software en el UC500. Pueden instalarse hasta dos idiomas, pero sólo un idioma de correo de voz puede estar activo en un momento determinado.

Configuración	Descripción
Fecha y hora	
Formato de fecha	Formato de fecha (dd-mm-aa, mm-dd-aa, aa-mm-dd, aa-dd-mm) para visualización por teléfono.
Formato de hora	Formato de hora (12 horas ó 24 horas) para visualización por teléfono
Otras configuraciones Esta sección muestra la localización del Plan de discado y de la Zona horaria seleccionados, junto con información acerca de dónde se configuran en CCA.	

10

Puertos y enlaces de voz

Esta sección cubre la configuración de puertos y enlaces de voz. Se analizan los siguientes temas:

- **Puertos FXS**
- **Enlaces PSTN**
- **Troncal SIP**
- **Estado de enlace**

Puertos FXS

Aparece la ventana Puertos FXS cuando se selecciona **Configurar** > **Telefonía** > **Puertos y enlaces** > **Puertos FXS** en la barra de funciones.

Visión general

En la ventana Puertos FXS de puertos analógicos, se define cómo se utilizarán los puertos FXS incorporados y se selecciona un tipo de señalización.

La configuración para los puertos de la tarjeta de interfaz de voz FXS/DID (VIC) se configuran en la sección Puertos y enlaces de la ventana Enlaces PSTN (consulte **FXS/DID (sólo VIC), página 312**). Si los puertos de la tarjeta de la interfaz de voz FXS se configura dentro de la configuración de Enlaces PSTN y luego la opción de perfil puede configurarse como Teléfono o facsímil de área común.

Procedimientos

Configure los Puertos FXS como se describe a continuación, luego haga clic en **Aceptar** para aplicar la configuración.

Configuración	Explicación
Puertos FXS	Sólo lectura. Muestra la ID del puerto FXS, por ejemplo, 0/0/0.
Perfil	Define cómo se utilizará el dispositivo conectado a este puerto FXS y dónde se configura. Realice una de las siguientes acciones: ▪ **Teléfono de usuario**. Permite que se configuren funciones avanzadas en el teléfono, como correo de voz. Los puertos se controlan por SCCP y ocupan una licencia de usuario. Las funciones disponibles se configuran en **Configurar** > **Telefonía** > **Usuarios y anexos** > **Usuarios y teléfonos** > **Anexos de usuarios**. ▪ **Teléfono de área común**. Un teléfono de área común es, típicamente, un teléfono analógico ubicado en un lobby o sala de descanso. Las funciones avanzadas, como correo de voz, desvío de llamadas, etc., no están disponibles en estos teléfonos. Los puertos FXS asignados a este perfil se configuran en la ficha Anexos analógicos de la ventana Usuarios y teléfonos (**Configurar** > **Telefonía** > **Usuarios y anexos** > **Usuario y teléfonos**). ▪ **Fax**. Permite la integración con funciones como troncal SIP o T.37 Facsímil a correo ya que se necesita una configuración adicional/especial para que ellos administren las máquinas de facsímil. (**Configurar** > **Telefonía** > **Usuarios y anexos** > **Usuarios y teléfonos**).
Descripción	*Opcional*. Especifique una descripción que identifique este puerto FXS y su utilización.
Señal	Seleccione **Inicio de retrobucle** o **Inicio desde cero** como el tipo de seña, dependiendo de lo que el proveedor de servicios solicite. El valor predeterminado es Inicio de retrobucle.

Configuración	Explicación
Anexo	Si se configura un anexo, se muestra aquí. Para configurar un anexo, seleccione **Configurar** >**Telefonía** > **Usuarios y anexos**> **Usuarios y teléfonos**. Si a este puerto se le asigna un perfil de Teléfono o facsímil de área común, seleccione la ficha Anexos analógicos e indique el anexo. Si a este puerto se le aigna un perfil de Teléfono de usuario, seleccione la ficha Anexos de usuarios, seleccione el teléfono y haga clic en **Editar**.

Enlaces PSTN

Para acceder a las opciones de configuracion del enlaces PSTN, seleccione **Configurar** > **Telefonía** > **Puertos y enlaces** > **Enlaces PSTN**. La configuración de enlaces PSTN también pueden configurarse por medio del Asistente de configuración de telefonía.

La configuración y opciones que se indican en las finas de la ventana Enlaces PSTN varían, dependiendo de los tipos de interfaces PSTN disponibles en la plataforma UC500 que se esté configurando.

Consulte las siguientes secciones para obtener información sobre la configuración de interfaces PSTN.

- **FXO**
- **Interfaz de velocidad básica (BRI)**
- **Interfaz T1/E1**
- **FXS/DID (sólo VIC)**

FXO

Si hay puertos FXO disponibles en el router, esta ficha muestra información de sólo lectura indicando el número de puertos FXO disponibles. Por ejemplo:
`Puertos totales: 4 (4 incorporados, 0 VIC)`

Para ver información acerca de la configuración de puertos FXO, consulte **Configuración de puertos FXO, página 313**.

Para obtener información acerca de la visualización del estado y administración de los puertos FXO, consulte **Estado de enlace, página 327**.

Interfaz de velocidad básica (BRI)

Si la Interfaz de velocidad básica (BRI) está presente en el sistema, defina la configuración como se describe en la siguiente tabla.

NOTA Si está presente y seleccionado el PRI de ISDN y si también está presentes una o más interfaces BRI, se debe configurar el tipo de switch de BRI. El parámetro Tipo de switch se utiliza para configurar el tipo de switch ISDN en la interfaz BRI para evitar conflictos.

Configuración	Descripción
Tipo de switch BRI	Seleccione uno de los siguientes tipos de switch BRI, según lo indique su proveedor de servicios: 5ESS básico, DMS100, NI básico, NTT, 1TR6 básico, NET3 básico, VN3, QSIG básico.
Capacidad del portador	Seleccione uno de los siguientes, según lo indique su proveedor de servicios: Ninguno, Hablar ó 3100 Hz.
TEI estática de ISDN	Seleccione Ninguno o seleccione un número para configurar estáticamente el valor del Identificador de punto final del terminal (TEI), según lo indique su proveedor de servicios. El valor de TEI representa cualquier dispositivo con capacidad ISDN adscritos a una red ISDN que estén en el punto final del terminal. Los TEI se utilizan para distinguir entre varios dispositivos diferentes utilizando los mismos enlaces ISDN.

Interfaz T1/E1

Si hay presente una interfaz T1/E1, determine la configuración según se describe en la siguiente tabla. Haga clic en **Aceptar** o **Aplicar** cuando haya finalizado.

En las plataformas UC560, pueden configurarse hasta dos (2) puertos T1/E1; estos pueden ser puertos en una interfaz T1/E1 incorporada o en una interfaz T1/E1 instalada en una ranura VIC.

Configuración	Descripción
Tipo de conexión	Haga clic en el botón de radio **Tipo de conexión** para seleccionar T1 ó E1. Esta configuración sólo está disponible para la configuración inicial. Después de configurar este parámetro, el campo queda de sólo lectura. Aparecen las opciones T1/E1 si el dispositivo tiene una interfaz T1/E1.
Señalización de canales	Realice una de las siguientes acciones: ▪ ISDN PRI ▪ FXO ▪ FXS ▪ E&M ▪ FGD

Configuración	Descripción
ISDN PRI	Si se seleccionó ISDN PRI como el tipo de señalización de canales, determine las siguientes configuraciones, según lo indique su proveedor de servicios. ▪ En el menú **Tipo de switch**, seleccione el tipo de switch que se va a configurar. Este parámetro se utiliza para configurar el tipo de switch ISDN global y el tipo de switch de nivel de interfaz. ▪ En el campo **Capacidad del portador**, seleccione Ninguno, Hablar ó 3100 Hz. ▪ En la selección **Grupo PRI**, especifique el intervalo de lasranuras de tiempo para el grupo de ISDN PRI. El intervalo T1 por defecto es de 1 a 24 ranuras de tiempo; siempre se incluye la ranura 24 (el canal D). El intervalo de tiempo desde la ranura 24 a la ranura 24 es inválido. El intervalo E1 por defecto es de 1 a 31 ranuras de tiempo; siempre se incluye la ranura 16 (el canal D). El intervalo de tiempo desde la ranura 16 a la ranura 16 es inválido.

Configuración	Descripción
FGD (Sólo se utiliza para T1)	Si seleccionó FGD en el menú Señalización de canales, realice estos pasos: ▪ Para seleccionar el tipo de señal, haga clic en EANA o en OS (servicios de operadora). ▪ Para utilizar ranuras de tiempo separadas para las llamadas entrantes y salientes, marque la casilla **Usar grupos separados para llamadas entrantes y salientes**. ▪ En los campos **Ranuras de tiempo**, especifique el intervalo de las ranuras de tiempo. Si se marcó la casilla **Utilizar grupos separados para llamadas entrantes y salientes**, especifique el intervalo de las ranuras entrantes en el campo **Ranuras de tiempo para grupo entrante** y especifique el intervalo de las ranuras salientes en el campo **Ranuras de tiempo para grupo saliente**. El intervalo T1 por defecto es de 1 a 24 ranuras de tiempo; siempre se incluye la ranura 24 (el canal D). El intervalo de tiempo desde la ranura 24 a la ranura 24 es inválido.

Configuración	Descripción
FXO **FXS** **E&M**	Si seleccionó FXO, FXS o E&M en el menú Señalización de canales, realice estos pasos: ▪ Seleccione el tipo de señal. ▪ Para utilizar ranuras de tiempo separadas para las llamadas entrantes y salientes, marque la casilla **Utilizar grupos separados para llamadas entrantes y salientes**. ▪ En los campos **Ranuras de tiempo**, especifique el intervalo de las ranuras de tiempo. Si se marcó la casilla **Utilizar grupos separados para llamadas entrantes y salientes**, especifique el intervalo de las ranuras entrantes en el campo **Ranuras de tiempo para grupo entrante** y especifique el intervalo de las ranuras salientes en el campo **Ranuras de tiempo para grupo saliente**. El intervalo T1 por defecto es de 1 ranura de tiempo hasta 24 ranuras de tiempo; para estos tipos de señalización T1, no hay canal D dedicado. El intervalo E1 por defecto es de 1 a 31 ranuras de tiempo; siempre se incluye la ranura 16 (el canal D). El intervalo de tiempo desde la ranura 16 a la ranura 16 es inválido.

FXS/DID (sólo VIC)

Si se encuentra presente una tarjeta de interfaz de voz (VIC) FXS/DID, determine las siguientes configuraciones para cada puerto.

NOTA: Para configurar puertos FXS*incorporados*, seleccione **Configurar** > **Telefonía**> **Puertos y enlaces**> **Puertos FXS** en la barra de funciones.

Configuración	Descripción
Modo	Seleccione FXS o DID

Configuración	Descripción
Señal	Si el Modo se configura como **FXS**, seleccione **Inicio de retrobucle** o **Inicio desde cero**, según lo indique su proveedor de servicios. Si el Modo se configura como **DID**, seleccione **Inmediato**, **Wink Start** o **Delay Start**, según lo indique su proveedor de servicios.
ID de quien llama	Si el Modo se configura como FXS, especifique el número que se mostrará para la ID de quien llama para este puerto FXS. N/A si el modo se configura como DID.
Anexo	Si el Modo se configura como FXS, especifique el número que se mostrará para el anexo de este puerto FXS. N/A si el modo se configura como DID.
Bloquear números restringidos	Si el modo de configura como **FXS**, haga clic en **Activar** o en **Desactivar**. N/A si el modo se configura como DID.
Permisos	Si el modo se configura como FXS, este campo es N/A y no editable hasta que se indiquen datos en los campos ID de quien llama y Anexo. Una vez llenos esos campos, se puede seleccionar **Nacional, Interno, Local, Internacional, Sin restricciones, Local-Plus** o **Nacional-Plus**. N/A si el modo se configura como DID.

Configuración de puertos FXO

Para navegar hasta el panel del enlace FXO en la barra de funciones, seleccione **Configurar** > **Telefonía** > **Puertos y enlaces** > **Enlaces PSTN** > **Ficha FXO**.

Edición de la configuración de puertos FXO

Para modificar la configuración general de los puertos o ajustar la configuración de audio y temporizadores para el puerto seleccionado, seleccione **Editar configuración.** (Si se hace doble clic en la fila seleccionada también se iniciará la ventana Editar configuración).

Las fichas de configuración de puertos FXO son:

- **Ficha General**
- **Fica Temporizadores**
- **Ficha Audio**

Ficha General

Para configurara los parámetros de la configuración general de los puertos, complete los campos como se describe en la siguiente tabla y luego, haga clic en **Aceptar** o **Aplicar**.

Comuníquese con el proveedor de servicios de las líneas CO para determinar cómo estos parámetros deben configurarse para un sitio en particular.

Configuración	Descripción
Tipo de señalización	Las interfaces FXO y FXS indican el estado de colgado o descolgado y la toma de líneas telefónicas ppor parte de uno de dos métodos de señalización: inicio en bucle o inicio desde cero. ▪ **Inicio en bucle**. Configura la señalización del inicio en bucle en el puerto seleccionado y usado específicamente para las interfaces de Oficina de intercambio remoto (FXO) y Estación de intercambio remoto (FXS). Con la señalización de inicio en bucle sólo un lado de una conexión puede colgar. Esta es la configuración por defecto para los puertos de voz FXO y FXS. ▪ **Inicio desde cero**. Configura la señalización de inicio desde cero en los puertos de voz y específicamente para las interfaces FXO y FXS. La señalización de inicio desde cero permite que ambos lados de una comunicación hagan una llamada y cuelguen.

Configuración	Descripción
Tipo Compansión	Especifica el estándard e compansión que se usa para convertir las señales analógicas y digitales en los sistemas de modulación por impulsos codificados (PCM). ▪ **u-law**. Configura el estándar de codificación de PCM como u-law ITU-T de Estados Unidos para un puerto en particular. Ésta es la configuración predeterminada. ▪ **a-law**. Configura el estándar de codificación de PCM como a-law ITU-T Europeo.
Desconexión supervisora	Se aplica sólo a la señalización de inicio en bucle y típicamente se usa para puertos de voz colgados. Las opciones de desconexión supervisora se desactivan cuando se selecciona Inicio desde cero como el tipo de señalización. Las opciones de desconexión supervisora son las siguientes: ▪ **Anytone** ▪ **Pre-conexión de tono doble** ▪ **Tono doble en mitad de llamada** ▪ **Señal** Esta es la opción por defecto de Desconexión supervisora para el puerto FXO. Comuníquese con el Centro de soporte para pequeñas empresas de Cisco para recibir ayuda. Para ver mayor información, seleccione **Solución de problemas** > **Información de soporte**.

Configuración	Descripción
Activar reversión de baterías	El comando de reversión de baterías se aplica a los puertos de voz FXO y FXS. Los puertos FXS normalmente reversan la batería al conectar la llamada. La opción Activar reversión de baterías restablece los puertos de voz a su operación de reversión de baterías por defecto. Si un puerto FXO o su par FXS no admiten la reversión de baterías, evite activar el comando de reversión de baterías en el puerto FXO. Por defecto, esta opción está marcada.

Fica Temporizadores

Para configurar los parámetros de los temporizadores, complete los campos como se describe en la siguiente tabla y luego, haga clic en **Aceptar** o **Aplicar**.

Configuración	Descripción
Búfer de fluctuación de paquetes	El retraso de reproducción es la cantidad de tiempo que transcurre entre el momento en que un paquete de voz se recibe en el búfer de fluctuación en el procesador de la señal digital (DSP) y el momento en que éste se reproduce en el códec.
	Modo: ▪ **Adaptivo**. Cuando el modo de retraso de reproducción se configura como Adaptativo, el tamaño del búfer de fluctuación y la cantidad del retraso se ajustan durante una llamada, basados en las condiciones presentes en la red. Es la opción por defecto para el modo de Retraso de reproducción. ▪ **Fijo**. Cuando el modo de Retraso de reproducción se configura como Fijo, el tamaño del búfer de fluctuación no se ajusta durantes una llamada, se agrega un retraso de reproducción constante.
	Nominal: Configura la hora de configuración inicial y el retraso mínimo permitido que el DSP puede insertar antes de reproducir paquetes de voz. El intervalo permitido es 40 - 250 milisegundos. El valor por defecto es 60 milisegundos.
Temporizador	Configura los valores de Desconexión supervisora para el puerto. Esta configuración se usa principalmente para asegurar que un indicio de colgado es interncional.
	Temporizador de Sup-Disconnect: El intervalo permitido es 50 - 1500 milisegundos. El valor por defecto es 350 milisegundos.

Configuración	Descripción
Límites de tiempo	Espera para liberación: Especifica el tiempo que un puerto de voz puede ser retenido en un estado de fallo de llamadas mientras el router de Cisco envía un tonno de ocupado, tono de reorden o un tono de fuera de servicio al puerto. Una vez que expira el límite de tiempo, se activa la secuencia de liberación. El intervalo permitido es 1 - 3600 milisegundos. La configuración por defecto es 30 segundos.
	Desconexión de llamada: Especifica la lapso durante el que un puerto de voz FXO permanece conectado luego que quien llama cuelga, cuando esa llamada no se contesta. El intervalo permitido es 0 - 120 milisegundos. La configuración por defecto es 60 segundos.

Ficha Audio

Para configurar los parámetros de audio, complete los campos como se describe en la siguiente tabla y luego, haga clic en **Aceptar** o **Aplicar**.

.

Configuración	Descripción
Cobertura de cola de eco	Configura la cobertura de cancelación de eco en el puerto de voz y se usa específicamente para ajustar el tamaño de la cobertura de la EC. Este comando activa la cancelación de voz que se envía a la interfaz y se recibe en la misma interfaz dentro del lapso configurado. Si el bucle local (la distancia desde la interfaz al equipo conectado que está produciendo el eco) es mayor que este lapso, el valor configurado para este comando debe aumentarse. El intervalo permitido para el paquete de software 8.0 y posteriores es [24 | 32 | 48 | 64 | 80 | 96 | 112 | 128] ms El intervalo permitio para todas las versiones previas del paquete de software es de 24 | 32 | 48 | 64 | ms El valor por defecto es 64 milisegundos.
	Activar Canal de eco: El comando de activación del canal de eco activa la cancelación de voz que se envía a la interfaz y que se recibe de vuelta en la misma interfaz; el sonido que se recibe de vuelta de esta forma se percibe como eco. Si se desactiva la cancelación de eco se podría ocasionar que se escuche un eco en el lado remoto de la conexión. Debido a que la cancelación de eco es un proceso invasivo que puede degradar mínimamente la calidad de voz, este comando debe desactivarse si no es necesario. El estado por defecto es desactivado. Este es un parámetro de configuración avanzado. Comuníquese con el Centro de soporte para pequeñas empresas de Cisco para recibir ayuda. Para ver mayor información, seleccione **Solución de problemas** > **Información de soporte**.

Configuración	Descripción
Cobertura de cola de eco (continuación)	Activación no lineal: Configura el comando no lineal en el puerto de voz y se usa, específicamente, junto con el comando de cancelación de eco. La función activada por este comando también se conooce como supresión de eco residual. El estado por defecto sólo se activa si la cancelación de eco está activada. Este es un parámetro de configuración avanzado. Comuníquese con el Centro de soporte para pequeñas empresas de Cisco para recibir ayuda. Para ver mayor información, seleccione **Solución de problemas** > **Información de soporte**.
Ganancia de entrada	Configura la ganancia de entrada en decibeles en los puertos de voz, específicamente, cuando el usuario desea aumentar la ganancia de una señal que entra al router. Si el nivel de voz es demasiado bajo, el usuario puede aumentar la ganancia de entrada nuevamente. El intervalo permitido es de -6 dB hasta +14 dB El valor por defecto es 0 dB.
Atenuación de salida	Configura el nivel de atenuación en decibeles en los puertos de voz, específicamente, cuando el usuario desea aumentar la atenuación de una señal que sale del router. Si el nivel de voz es demasiado alto, el usuario puede aumentar la atenuación. Si el nivel de voz es demasiado bajo, el usuario puede reducir la atenuación. El intervalo permitido es de -6 dB hasta +14 dB El valor por defecto es 3 dB.

Configuración	Descripción
Impedancia	Esta configuración especifica la impedancia terminal de las interfaces de telefonía analógica. Para ajustar la impedancia, seleccione una de las siguientes opciones. ▪ **600c.** 600 ohms + 2.15 uF ▪ **600r.** Terminación resistiva de 600 ohm ▪ **900c.** 900 ohms + 2.15 uF ▪ **900r.** Terminación resistiva de 900 ohm ▪ **Complex 1.** 220 ohms + (820 ohms || 115 nF) ▪ **Complex 2**. 270 ohms + (750 ohms || 150 nF) ▪ **Complex 3.** 370 ohms + (620 ohms || 310 nF) ▪ **Complex 4.** 600r, línea = 270 ohms + (750 ohms || 150 nF) ▪ **Complex 5.** 320 + (1050 ohms | 230 nF), línea = 12 Kft ▪ **Complex 6.** 600r, línea = 350 ohms + (1000 ohms || 210 nF) La impedancia por defecto es específica para cada país. En norteamérica, el valor por defecto es de 600r.

Copia de la configuración de puertos FXO

Para copiar todas las configuraciones de puertos de un puerto a otros, seleccione estos pasos.

PASO 1 En la ventana de la ficha FXO, haga clic en la fila de la tabla que corresponda al puerto que desea copiar.

PASO 2 Haga clic en **copiar configuración**. Un puerto FXO copia ventana de Configuración, lista configuración del puerto y sus valores correspondientes, se abrirá.

PASO 3 En la sección Copiar configuración a de la ventana, seleccione el o los puertos FXO que desea copiar a la configuración copiada, y haga clic en **Agregar**.

La lista Puertos disponibles está vacía si todos los puertos tienen configuraciones idénticas.

- Haga clic en **Seleccionar todo** para seleccionar todos los puertos FXO disponibles.
- Haga clic en **Eliminar** para eliminar un puerto FXO de la lista.

PASO 4 Haga clic en **Aceptar**.

PASO 5 En la ventana de la ficha FXO haga clic en **Acpetar** o en **Aplicar** para completar la copia de los cambios en las configuraciones.

Troncal SIP

Para configurar la configuración del troncal SIP, seleccione **Configurar** > **Telefonía** > **Puertos y enlaces** > **Troncal SIP** en la barra de funciones.

Se analizan los siguientes temas:

- **Visión general**
- **Ficha Troncal SIP**
- **Configuración del Proveedor genérico de troncal SIP**
- **Ficha Opciones avanzadas**

Visión general

Los parámetros del troncal SIP configurados en esta ventana varían dependiendo de la plantilla del proveedor de servicios seleccionado. Los valores de los parámetros del troncal SIP deben obtenerse del proveedor de Servicios de telefonía por internet (ITSP).

Si su ITSP no está indicado, use la plantilla para el Proveedor SIP genérico para configurar el troncal SIP. Para obtener mayor información sobre la configuración que CCA define automáticamente usando esta plantilla, consulte **Configuración del Proveedor genérico de troncal SIP, página 326**.

En la ficha Opciones avanzadas, se puede especificar las direcciones IP a las que se les permite acceder a su red de VoIP.

Para saber más sobre los Enlaces SIP en las plataformas SBCS/UC500 de Cisco, visite el siguiente enlace en la Comunidad de soporte para pequeñas empresas de Cisco:

https://supportforums.cisco.com/docs/DOC-9830/

Ficha Troncal SIP

Para configurar los parámetros del troncal SIP, complete los campos como se describe en la siguiente tabla y luego, haga clic en **Aceptar** o **Aplicar**.

Campo	Descripción
Proveedor de servicio	El proveedor de servicios del troncal SIP al que se conectará este router para el acceso PSTN. Los proveedores de servicios SIP certificados por Cisco se identifican en la lista desplegable de Proveedores de servicios con el logo de Cisco. Para configurar los parámetros del troncal SIP para otros proveedores, seleccione **Proveedor genérico de troncal SIP** en la lista desplegable de Proveedores de servicios y complete los campos que ese Proveedor de servicio solicite. Para obtener mayor información sobre la configuración del Proveedor genérico de troncal SIP, consulte **Configuración del Proveedor genérico de troncal SIP, página 326**. Las opciones **Agregar** y **Eliminar** de la lista desplegable de Proveedores de servicios se entregan para que puedan importarse o eliminarse las plantillas personalizadas de Proveedores de servicios. ▪ Las plantillas incorporadas para los Proveedores de servicios certificados por Cisco no pueden eliminarse. ▪ Las plantillas que se van a importar se obtienen del Proveedor de servicio SIP. Cuando se agrega una nueva plantilla de Proveedor de servicio, queda disponible para su selección en la lista de Proveedores de servicios y la adecuada configuración específica para Proveedores de servicios aparece cuándo éste se selecciona. Para las plantillas personalizadas, se muestra la información de versión y la marca horaria.

Campo	Descripción
Servidor proxy (primario)	Dirección IP o nombre de host DNS del servidor proxy SIP primario para el ITSP.
Servidor proxy (secundario)	*Opcional*. Dirección IP o nombre de host DNS del servidor proxy SIP secundario (de copia de seguridad) para el ITSP.
Servidor de registro	*Opcional*. Dirección IP o nombre de host DNS del servidor de registro SIP para el ITSP. Este campo es obligatorio si el ITSP necesita registros SIP.
Servidor proxy saliente	*Opcional*. Dirección IP o nombre de host DNS del Controlador de bordes de sesión (SBC) para el ITSP. Esta configuración es necesaria si la dirección IP del SBCS en el ITSP no es la misma que la del servidor de proxy SIP.
Número máximo de llamadas	*Opcional*. Número de llamadas concurrentes admitidas para el control de admisión de llamadas. Debe configurar estos parámetros si el ITSP requiere que el UC500 limite el número de llamadas concurrentes. Verifique con su ITSP para ver si es necesaria esta configuración. El intervalo para el número admitido de llamadas concurrentes se indica entre paréntesis cuadrados, por ejemplo [1-48]. El número máximo de llamadas concurrentes es igual al número de licencias en el UC500. Cuando se cambia esta configuración, la configuración Máximo de llamadas en **Configurar** > **Telefonía** > **Máximo Llamadas** también se actualiza. Consulte **Máximo de llamadas (Control de admisión de llamadas), página 518**.
Empresa	*Opcional*. Nombre de la empresa del cliente que se va a usar para la ID de quien llama. Este campo es obligatorio si debe indicarse una ID de quien llama para las llamadas salientes. En la mayoría de casos, esto lo administra el ITSP. Verifique con su ITSP para ver si es necesaria esta configuración. Este valor se inserta en el encabezado de la invitación SIP.

Campo	Descripción
Autenticación Digest	*Opcional*. **Nombre de usuario** y **Contraseña** para la el registro o llamadas SIP. Esta configuración es obligatoria si hay un servidor de Registro SIP presente. Haga clic en la casilla **Mostrar contraseña como texto plano** para cambiar la visualización de la contraseña en texto plano.
Servicio de nombre de dominio	*Opcional.* **Nombre de dominio.** Nombre del dominio para el servidor SIP. El nombre del dominio SIP es específico para los servicios de Voz sobre IP (VoIP). *Opcional.* **Dirección del servidor DNS**. Dirección IP del servidor DNss para el dominio SIP. Se puede configurar un servidor DNS aquí si no hay un servidor DNS configurado y los nombres de dominio se está utilizando para la configuración del troncal SIP. Sin embargo, la ubicación preferida para la configuración DNS está en la ficha Configuración del dispositivo de la ventana Direcciones IP (**Configurar** > **Ruteo** > **Direcciones IP**).
Credenciales de usuario	*Opcional*. Este campo es necesario si el ITSP necesita un registro SIP con un nombre de usuario y contraseña únicos por cada DID asociada al UC500. La mayoría de los ITSP sólo registrar el número principal. Para agregar un conjuntos de credenciales de usuario para los ISTP que soliciten autenticacion SIP por DID: 1. Haga clic en **Agregar** para crear una nueva fila en la tabla. 2. Haga clic en la columna **Nombre de usuario** para la nueva fila y especifique un nombre de usuario. En general, el campo nombre de usuario contendrá un número PSTN en formato E.164. 3. Haga clic en la columna **Contraseña** de la nueva fila y especifique la contraseña que el ITSP entregó. 4. Haga clic en la casilla **Especificar contraseña como texto plano** para cambiar la visualización de las contraseñas de usuarios en texto plano. 5. Repita estos pasos para agregar más credenciales.

Para eliminar un conjunto de credenciales de usuario SIP por DID, siga estos pasos:

PASO 1 Haga clic en la fila de la tabla que corresponda al conjunto de credenciales que desee eliminar.

PASO 2 Haga clic en **Eliminar.**

PASO 3 Haga clic en **Aplicar.**

Configuración del Proveedor genérico de troncal SIP

Cuando se selecciona **Proveedor genérico de troncal SIP** para la plantilla del proveedor SIP, CCA muestra todas las opciones configurables para los enlaces SIP.

Además de las opciones de configuración, CCA automáticamente configura esta configuración en los enlaces SIP configurados usando la plantilla genérica:

- **Códec de voz**: G.711-ulaw
- **Códec de fax**: G.711
- **Carga útil de DTMF (tono dual de multi-frecuencia)**: 101
- **Registro SIP**: Registra sólo el número principal

La plantilla del Proveedor genérico de troncal SIP no es compatible con todos los ITSP. Para solicitar una plantilla CCA para un nuevo Proveedor SIP, vaya al siguiente enlace oen la Comunidad de soporte para pequeñas empresas de Cisco:

https://supportforums.cisco.com/docs/DOC-9685/

Ficha Opciones avanzadas

Por motivos de seguridad, CCA bloquea el tráfico SIP desde fuentes desconocidas. Configure direcciones IP adicionales aquí si su proveedor de servicios utiliza gateways SIP con direcciones IP que sean diferentes de los servidores proxy configurados en la ficha Enlaces SIP.

Consulte su proveedor SIP para conocer las direcciones de los gateways SIP que utilicen.

Para configurar direcciones IP adicionales a las que se les permite acceso a la red VoIP, siga estos pasos.

PASO 1 Haga clic en **Agregar** para abrir una nueva una fila en la tabla para su edición.

PASO 2 Especifique la dirección IP.

PASO 3 Configure direcciones IP adicionales, si es necesario.

PASO 4 Haga clic en **Aceptar**.

Estado de enlace

La ventana Estado del enlace de voz aparece cuando se selecciona **Configurar** > **Telefonía** > **Puertos y enaleces**>**Enlace de voz** en la barra de funciones.

Visión general

En la ventana Estado de enlace, se puede ver Puerto de enlace, Estado actual y Acción.

En la ventana desplegable Acción, se puede desconectar los puertos inactivos. Esto asegura que las llamadas no se envían a los puertos seleccionados si no hay dispositivos conectados.

Cuando se apaga un puerto de voz, no se le pueden enviar llamadas. Sin embargo, el puerto aún aparece como una opción disponibles en otras pantallas de Configuration Assistant. La configuración aún puede aplicarse al puerto, pero el puerto debe reacitvarse
manualmente antes de poder comenzar a usar esa configuración.

Procedimientos

Para apagar o restablecer un puerto de enlace de voz, seleccione el puerto de la lista y seleccione **Restablecer puerto** o **Apagar puerto** del menú desplegable en la columna Acción. Luego, haga clic en **Aplicar** o en **Aceptar**.

Para reactivar un enlace de voz que se apagó, seleccione el puerto de la lista y seleccione **Activar puerto** del menú desplegable en la columna Acción. Luego, haga clic en **Aplicar** o en **Aceptar**.

11

Usuarios y anexos

Esta sección explica cómo realizar la configuración de usuarios, teléfonos y anexos que se indican en **Configurar** > **Telefonía** > **Usuarios y anexos** en la barra de funciones.

Se analizan los siguientes temas:

- **Usuarios y teléfonos**
- **Correo de voz y notificaciones**
- **Ubicación con número individual (SNR)**
- **Discados rápidos del sistema**

Usuarios y teléfonos

Para abrir la ventana Usuarios y teléfonos, seleccione **Configurar** > **Telefonía** > **Usuarios y anexos** > **Usuarios y teléfonos** en la barra de funciones.

Consulte las siguiente secciones para obtener más información acerca de la configuración de las opciones en cada una de las fichas de la ventana Usuarios y teléfonos:

- **Anexos de usuarios**
- **Anexos flotantes**
- **Movilidad de anexos**
- **Anexos analógicos**
- **Configuración de asignaciones de botones de teléfonos**

Anexos de usuarios

Siga las instrucciones de esta sección para:

- **Agregar, editar y eliminar teléfonos**
- **Importación de datos de teléfonos para múltiples usuarios (Importación de usuarios a granel)**

SUGERENCIA Haga clic con el botón izquierdo y arrastre el ratón sobre los encabezados de columnas para ordenar las columnas de la vista. También puede hacer clic con el botón izquierdo en el encabezado de las columnas de la vista para ordenar los datos en orden ascendente o descendente.

Agregar, editar y eliminar teléfonos

Cuando se conecte un teléfono IP al UC500, éste se registrará automáticamente y se le asignará una dirección IP en la VLAN de voz (VLAN100) usando DHCP. La dirección MAC del teléfono también se descubre y se muestra.

También puede agregar teléfonos sin registrar y realizar su configuración. Luego, cuando el teléfono esté conectado, recibirá su configuración.

Los usuarios y anexos para los teléfonos conectados a puertos FXS a los que se les asigna un perfil de Teléfono de usuario también se configuran aquí.

Para ver instrucciones paso a paso, consulte estas secciones:

- **Cómo agregar un teléfono**
- **Cómo editar un teléfono**
- **Cómo eliminar un teléfono**

Si se está agregando y pre-configurando una gran cantidad de teléfonos, se realiza una importación a granel de datos de usuarios y teléfonos. Para ver instrucciones sobre cómo realizar una importación a granel, consulte **Importación de datos de teléfonos para múltiples usuarios (Importación de usuarios a granel), página 336**.

Cómo agregar un teléfono

Puede agregar un teléfono y preconfigurarlo antes que se conecte físicamente al sistema.

Para agregar un teléfono y asociar un usuario con el teléfono, siga estos pasos.

PASO 1 En la ventana Usuarios y teléfonos, haga clic en el botón **Agregar** en la parte inferior de la ventana.

PASO 2 Realice esta configuración para el nuevo teléfono.

Campo	Descripción
Información de teléfono	
Dirección MAC	Escriba la dirección MAC para este teléfono IP.
Tipo de teléfono	Seleccione el modelo del teléfono IP de la lista desplegable. Cuando se selecciona un tipo de teléfono, la ficha Asignación de botones se actualiza para visualizar el número correcto de filas para el modelo seleccionado.
Módulo de expansión	*Opcional*. Para los teléfonos que admiten módulos de expansión, el menú **Módulo de expansión** indica los modelos admitidos. CCA no descubre automáticamente los módulos de expansión que están conectados a los teléfonos. Si uno o más módulos de expansión están conectados a un teléfono, debe seleccionarlos manualmente aquí. El "x2" selecciones en la lista indican que dos módulos de expansión se conectan al teléfono. Cuando seleccione un módulo de expansión de la lista, se agregan filas al la lista de botones para que los botones de línea en el módulo de expansión y actualizaciones gráficas del modelo de teléfono muestren el módulo de expansión.

Campo	Descripción
Permitir llamadas de vídeo	Seleccione si se permiten las llamadas con vídeo para este teléfono. La configuración **Permitir llamadas con vídeo** no se aplica a los teléfonos análogos ni a los ATA. ▪ Cuando se marca **Permitir llamadas con vídeo**, se activa Cisco Unified Voice Advantage (CUVA) para el teléfono de este usuario. Cuando se combina con una cámara de vídeo USB, CUVA permite que una PC conectada a un teléfono IP de Cisco Unified o a Cisco IP Communicator agregue vídeo a las llamadas internas realizadas en el teléfono. ▪ Cuando se desmarca **Permitir llamadas con vídeo**, las llamadas de vídeo no se permiten en este teléfono. Si esta configuración se ha modificaco de su valor original, éste valor se conserva si se cambia el Tipo de teléfono. En la mayoría de los casos, sólo se cambiará el Tipo de teléfono al agregar un teléfono no registrado. Si éste es el caso, se debe editar manualmente esta configuración después de cambiar el Tipo de teléfono. Pr defecto,**Permitir llamadas con vídeo** está inicialmente desmarcada. **NOTA** Los teléfonos IP de las series SPA300 y SPA500 no admiten llamadas con vídeo.

Campo	Descripción
Uso como teléfono de teletrabajo	Marque o desmarque la opción **Usar como teléfono de teletrabajo** para activar o desactivar MTP. Cuando se marca **Usar como teléfono de teletrabajo**, se configura el Punto de terminación de medios (MTP) en el teléfono para que Cisco Unified CME termine el flujo de medios. La configuración de MTP hace que el UC500 actúe como proxy. Los paquetes de medios se reenvían a otros teléfonos IP con la dirección IP del UC500 en el campo de direcciones fuente. MTP se usa, típicamente, en implementaciones de teléfonos de teletrabajo remotos. Cuano se desmarca esta opción, no se configura MTP en el teléfono. La casilla de verificación **Usar como teléfono de teletrabajo** no se muestra para los softphones de Cisco IP Communicator (CIPC), ya que MTP siempre se configura para los softphones CIPC.
Información del usuario	
Apellido	Apellido del usuario del teléfono. El apellido aparece en el directorio y se usa para el servicio Discado por nombre de la contestadora automática.
Primero Nombre	Primero nombre del usuario del teléfono. El primero nombre aparece en el directorio y se usa para el servicio Discado por nombre de la contestadora automática.
ID de usuario	ID del usuario para este usuario telefónico. Esta ID se utiliza cuando se inicia sesión en las páginas web de Opciones de usuario de Cisco Unity Express para cambiar la configuración telefónica.

Campo	Descripción
Contraseña	Contraseña para este teléfono IP. La contraseña es obligatoria si está activado el correo de voz, y es opcional si esta función está desactivada. Esta contraseña la utiliza el usuario telefónico para iniciar sesión en las páginas web de Opciones de usuario de Cisco Unity Express para cambiar la configuración del teléfono. La contraseña se aplica sólo a la GUI de Unity Express de Cisco y al Protocolo de acceso a mensajes a través de internet (IMAP). Si es un teléfono SCCP, este campo también se aplica a la GUI de Unified Communications Manager Express (CME) de Cisco.
Movilidad de anexos	
Activar movilidad de anexos	Cuando se marca esta casilla, se activa la función Movilidad de anexos para este teléfono. La casilla de verificación está activada sólo cuando existe un mínimo de un perfil de teléfono configurado y disponible. Para obtener más información, consulte **Movilidad de anexos, página 345**. **PRECAUCIÓN** Si se trata de un usuario existente, su configuración de buzón de correo de voz, asignaciones de botones, discados rápidos y teléfono se eliminarán y se sobreescribirán con el perfil seleccionado cuando se haga clic en Aceptar.
Perfil de cerrar sesión seleccionado	Choose a phone logout profile to apply to this user's phone. Para obtener más información, consulte **Movilidad de anexos, página 345**. El perfil del teléfono define la asignación de botones por defecto del teléfono cuando no hay inicio de sesión de usuarios de Movilidad de anexos.

Campo	Descripción
Asignaciones de botones de teléfonos y discado rápido	
Asignaciones de botones	Para cada botón del teléfono que desee configurar, seleccione un **Tipo de botón**. Se debe seleccionar un **Tipo de teléfono** antes de poder configurar Asignaciones de botones. El áre del **Botón <#>** de la página muestra la configuración que debe realizarse para el tipo de botón seleccionado. Para obtener información detallada acerca de los tipos de botones que pueden asignarse a cada tipo de botón y su configuración asociada, consulte **Configuración de asignaciones de botones de teléfonos, página 358**.
Discado rápido	Haga clic en la ficha **Discado rápido** para configurar el discado rápido para el teléfono. Para obtener más información, consulte **Discado rápido, página 339**.

PASO 3 Haga clic en **Aceptar**.

Cómo editar un teléfono

Una vez que se haya agregado un teléfono, siga los pasos de esta sección para editar la configuración del teléfono.

Cuando un teléfono está físicamente conectado al UC500, se descubre y se indica según su dirección MAC. No recibe un anexo automáticamente ni ninguna información de usuarios por defecto. Se debe editar el teléfono y realizar su configuración.

IMPORTANTE En versiones de CCA anteriores a 3.0, los teléfonos se asignaron automáticamente a un anexo y algo de información del usuario, pero ya no es el caso. Se debe editar la configuración del teléfono para agregar la configuración necesaria después de conectar los teléfonos.

Cuando se selecciona la ficha Anexos de usuarios inicialmente, muestra una lista de todos los teléfonos de usuarios. Puertos analógicos configurados con un perfil de Teléfono de usuario se indican en la página Anexos del usuario como Teléfonos analógicos. La dirección MAC, modelo del teléfono, primer anexo, nombre y apellido del usuario y la ID de éste se muestran para cada teléfono.

Para editar la configuración de un teléfono, siga estos pasos:

PASO 1 Haga clic en un teléfono para seleccionarlo, y haga clic en el botón **Editar** de la parte inferior de la ventana para visualizar sus detalles. También puede hacer doble clic en un teléfono de la lista para ver sus detalles y poder editarlos.

PASO 2 Edite la configuración según sea necesario. Para ver más información acerca de las configuraciones de teléfonos, consulte **Cómo agregar un teléfono, página 330**.

PASO 3 Haga clic en **Aceptar** para enviar la configuración al dispositivo.

Cómo eliminar un teléfono

Para eliminar uno o más teléfonos, siga estos pasos:

PASO 1 Desconecte los teléfonos que se van a eliminar.

PASO 2 Seleccione **Configurar** > **Telefonía** > **Usuarios y anexos** > **Usuarios y teléfonos** en la barra de funciones.

PASO 3 En la ventana Usuarios y anexos, haga clic en los teléfonos que desea eliminar para seleccionarlos.

PASO 4 Haga clic en **Eliminar**. Se eliminan todos los teléfonos seleccionados.

Importación de datos de teléfonos para múltiples usuarios (Importación de usuarios a granel)

Se entrega un archivo de Microsoft Excel de muestra, llamado BulkUserImport.xls, para ingresar los datos de teléfonos para múltiples usuarios. Estos datos pueden exportarse a XML e importarse en CCA.

Si se instaló Configuration Assistant en la ubicación por defecto, la ubicación del archivo es el siguiente directorio:

C:\Archivos de programa\Cisco Systems\CiscoSMB\Cisco Configuration Assistant\appdata

Para importar datos para múltiples teléfonos y usuarios hacia CCA, siga estos pasos.

PASO 1 En su PC, ubique el archivo Excel llamado `BulkUserImport.xls` en el directorio appdata del directorio de instalación de CCA en su PC.

PASO 2 Haga clic en **Activar Macros** cuando se le solicite hacerlo. Para que la importación funcione correctamente, deben estar activados los macros.

PASO 3 Haga una copia del archivo y dele un nombre diferente.

PASO 4 Abra el archivo y escriba la información necesaria en el archivo .XSL. Todos los datos indicados deben estar dentro de la tabla que se entrega en la planilla de cálculo.

Nombre del campo	Descripción
ID de usuario	*Obligatorio*. ID del usuario que se asociará a este teléfono.
Nombre Apellido	*Obligatorio*. Nombre y apellido del usuario asociado con este teléfono. El nombre y apellido pueden verse en el teléfono, usarse para discado por anexo en la Contestadora automática y se incluyen en las listas del directorio.
Tipo de teléfono	*Obligatorio*. En la lista desplegable, seleccione el modelo del teléfono. Seleccione la opción /14 si se conectará un módulo de expansión al teléfono. Marque la selección /14x2 si se conectarán dos módulos de expansión.
Dirección MAC	*Obligatorio*. Escriba la dirección MAC del teléfono en el siguiente formato: *nnnn.nnnn.nnnn* (por ejemplo, ABCD.1234.1234).
Anexo	*Obligatorio*. Escriba el número del anexo que se usará para el primer anexo en el teléfono (botón 1). El número de dígitos debe coincidir con la longitud del anexo seleccionado para el sitio (no se admiten anexos con longitud variable)
Contraseña	*Obligatorio*. Contraseña del usuario para este teléfono.

Nombre del campo	Descripción
Tipo de línea	*Obligatorio*. Seleccione Dual u Octal de la lista desplegable.
Anxo CFNA	*Obligatorio*. El número de teléfono externo o el anexo externo que se usará como destino para las llamadas no contestadas en el primer (primario) anexo. Al especificar un número externo, escriba el número exactamente como se marcará en su sistema, incluyendo códigos de acceso.
Anxo CFB	*Obligatorio*. El número de teléfono externo o el anexo externo que se usará como destino para las llamadas cuando el primer (primario) anexo está ocupado. Al especificar un número externo, escriba el número exactamente como se marcará en su sistema, incluyendo códigos de acceso.
Límite de tiempo de CFNA	*Obligatorio*. Número de segundos antes que las llamadas no contestadas se transfieran al destino CFNA. Por defecto, son 20 segundos.

PASO 5 Haga clic en el botón **Generar XML** en el archivo .XLS para exportar y guardar los datos en un archivo XML.

Puede darle el nombre que desee al archivo .XML, pero debe tener una extensión .XML.

PASO 6 Inicie CCA y avance hasta **Configurar** > **Telefonía** > **Usuarios y anexos** > **Usuarios y teléfonos**.

PASO 7 En la ventana Usuarios y teléfonos, haga clic en el botón **Importar** en la parte inferior de la ventana.

PASO 8 Haga clic en **Explorar** y avance hasta la ubicación del archivo .XML en su PC que contenga los datos generados del teléfono y usuarios.

PASO 9 Haga clic en **Aceptar** para cargar el archivo. CCA valida los datos XML cuando se importa el archivo.

PASO 10 Si existen errores, primero deben solucionarse en el archivo .XML, volver a generar el XML y luego
volver a importar el archivo .XML al CCA.

PASO 11 Cuando termine, haga clic en **Aceptar**.

Discado rápido

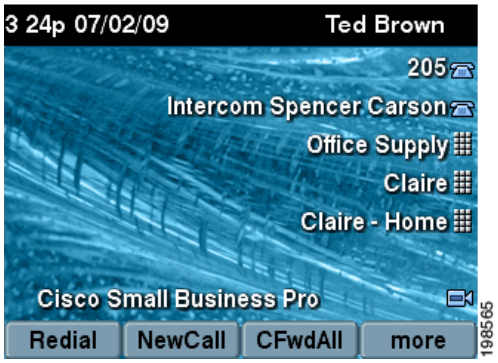
Para obtener información sobre la configuración de velocidad de marca personal en los teléfonos de usuarios o perfiles EM, vea las siguientes secciones:

- **Visión general**
- **Procedimientos**

Visión general

Se puede configurar discados rápidos personales para teléfonos individuales, teléfonos de Movilidad de anexos (por medio del Perfil de teléfono EM) y usuarios de Movilidad de anexos (por medio del Perfil del usuario EM). Estos discados rápidos se obtienen al presionar botones en el teléfono o desde menús en el teléfono IP.

Por ejemplo, el usuario Ted Brown tiene 205 como su anexo primario, un intercomunicador en el botón 2 y tres discados rápidos personales configurados en este teléfono. Los botones
3 a 5 muestran los discados rápidos personales.



Se aplican las siguientes pautas de utilización a los discados rápidos configurados desde esta ventana:

- Pueden configurarse hasta 55 discados rápidos.
- Estos números de discado rápido se aplican en orden, comenzando con el primer botón disponible en el teléfono del usuario.

- Los botones de discado rápido no pueden ubicarse entre los botones de líneas o de funciones. Por ejemplo, si el botón 1 se configura como anexo Normal y el botón 3 se configura como un botón de intercomunicador, el primer discado rápido se asigna al botón 4. Un discado rápido no puede asignarse al botón 2. Esto también se aplica a las asignaciones de botones para los teléfonos con módulos de expansión.
- Si el número de discado rápido configurado es mayor que el número de botones en el teléfono IP del usuario, el usuario del teléfono puede acceder al resto de los discados rápidos de los menús de su teléfono IP. Para acceder a estos discados rápidos:
  - Presionar el botón **servicios** en el teléfono IP.
  - En el menú URL de servicio CME, seleccione **Aplicaciones de mi teléfono**.
  - En el menú Aplicaciones de mi teléfono, seleccione **Botones de discado rápido**.
- Un usuario de teléfono IP también puede utilizar funciones de discado abreviado con estos discados rápidos. Para utilizar el discado abreviado:
  - Con el teléfono colgado, presione el número del discado de velocidad mientras aparece en la lista del menú. Por ejemplo, para marcar el discado rápido décimo en la lista, el usuario presiona "1" y luego "0."
  - Presione la tecla **AbbrDial** para marcar el número.
- Los discados rápidos que el usuario manualmente agregue desde el menú **servicios** a su teléfono también se muestra en la ventana Discados rápidos personales de CCA.
- Los teléfonos IP se reinician automáticamente después que se aplica la configuración de discado rápido.

Procedimientos

Para agregar, editar o eliminar los discados rápidos, para los teléfonos individuales o perfiles EM, siga estos pasos:

PASO 1 Seleccione **Configurar** > **Telefonía** > **Usuarios y anexos** >**Usuarios y teléfonos** en la barra de funciones.

PASO 2 Para configurar discados rápidos para un usuario de teléfonos regular, seleccione la ficha Anexos de usuarios en la ventana Usuarios y teléfonos.

Para configurar discados rápidos para un usuario de Movilidad de anexo o un perfil de teléfonos, seleccione la ficha Movilidad de anexos, la ficha Perfil del usuario o Perfil del teléfono y haga clic en la ficha Discados rápidos.

PASO 3 Haga clic en una fila de la tabla para seleccionar un teléfono para el que desee configurar discados rápidos.

Se puede clasificar los teléfonos en la lista según su anexo, tipo de teléfono, nombre, apellido, ID de usuario o dirección MAC.

PASO 4 Haga clic en **Editar**. Aparecerá la ventana Editar teléfono.

PASO 5 En la ventana Editar teléfono, seleccione la ficha Discado rápido.

PASO 6 En la ficha Discado rápido, siga estos pasos para agregar un discado rápido.

a. Haga clic en la fila que corresponda al número del botón de discado rápido que desee agregar o editar.

b. En el campo **Número**, especifique un número telefónico exactamente como el usuario lo marcaría, incluyendo un código de acceso para discado interno o prefijo de discado del sitio, si es necesario.

   Los caracteres del Este asiático de doble-byte *no* se admiten con los discados rápidos personales.

   El campo **Número** acepta los siguientes caracteres: dígitos 0-9, A, B, C, D, #, * y +. Los caracteres que no sean dígitos pueden usarse para acceso de seguridad u otros sistemas que un cliente pueda tener en su sitio.

c. En el campo **Etiqueta**, especifique una etiqueta para identificar el botón de discado rápido en la pantalla del teléfono.

PASO 7 Siga agregando botones de discado rápido según sea necesario.

PASO 8 Haga clic en **Aceptar** cuando termine.

PASO 9 Los teléfonos afectos se reinician automáticamente. Los teléfonos IP que están en usop se reinician después que se completga la llamada actual.

PASO 10 Para eliminar un discado rápido, siga estos pasos:

a. Haga clic en la fila que corresponda al número del botón de discado rápido que desee elliminar.

b. En el campo **Número**, elimine manualmente el número de teléfono.

c. En el campo **Etiqueta**, elimine manualmente los datos.

PASO 11 Haga clic en **Aceptar** cuando termine.

Los teléfonos afectos se reinician automáticamente. Los teléfonos IP que están en usop se reinician después que se completga la llamada actual.

Anexos flotantes

Para acceder a las configuraciones para los Anexos flotantes, vaya a **Configurar** > **Telefonía** > **Usuarios y anexos** > **Usuarios y teléfonos** y seleccione la ficha Anexos flotantes.

Visión general

Un anexo flotante es un anexo que no está asociado con ningún teléfono. A continuación se encuentran algunos ejemplos de cómo puede usarse esta función.

- Puede usar los anexos flotantes para crear buzones de correo de voz que no están asociados a ningún teléfono. Los usuarios pueden acceder a su correo de voz desde cualquier teléfono del sistema simplemente marcando el anexo del correo de voz o el número de acceso PSTN al correo de voz. Se les solicitará indicar su PIN de correo de voz. El PIN por defecto para el acceso al correo de voz es 1234. Los usuarios que accedan a su correo de voz por primera vez deberán cambir su PIN.
- Se puede configurar un anexo flotante para un trabajador móvil y configurarlo para que reenvíe todas las llamadas a su teléfono celular.

  El número reenviado puede cambiarse sin tener que cambiar el número del anexo, y el número real (en este caso, su teléfono celular) no queda expuerto para quien llama.

Puede mapear un número de DID hacia un anexo flotante en la ficha Discado directo de la ventana Plan de numeración entrante (**Configurar** > **Telefonía** > **Plan de numeración** > **Entrante**).

Un anexo flotante puede asignarse como:

- Un anexo de atención nocturna.
- Un destino de **Desvío sin respuesta** para las llamadas a un grupo de búsqueda. En la lista desplegable **Desvío sin respuesta**, seleccione **Otro número** y escriba el número del anexo flotante.

- Un destino para las llamadas transferidas desde la contestadora automática. Seleccione **Llamar a otro número**y escriba el número del anexo flotante.

Procedimientos

Para agregar o editar un anexo flotante, siga estos pasos:

PASO 1 Seleccione **Configurar** > **Telefonía** > **Usuarios y anexos** >**Usuarios y teléfonos**.

PASO 2 Seleccione la ficha Anexos flotantes.

PASO 3 Haga clic en **Agregar** o seleccione un anexo flotante existente de la lista y haga clic en **Editar**. Aparecerá la ventana Agregar/editar anexos flotantes.

PASO 4 Realice la configuración como se describe en **Cómo agregar o editar anexos flotantes**.

PASO 5 Haga clic en **Aceptar**.

Cómo agregar o editar anexos flotantes

Para crear un anexo que no esté asociado con ningún teléfono, realice la configuración como se describe a continuación, luego haga clic en **Aceptar**.

Configuración	Descripción
Configuración de anexo	
Número	Número del anexo que usará el anexo flotante. El anexo debe ser único y debe contener el número correcto de dígitos para su sistema.

Configuración	Descripción
Número PSTN	Si un número DID se ha mapeado a este anexo, se muestra aquí. Si no, el texto "No DID asignado" aparece. Para asociar un número DID a un anexo, vaya a **Configurar** > **Telefonía** > **Plan de numeración** > **Entrante** y seleccione la ficha Discado directo. En la sección Discado directo a anexos internos de la página, haga clic en **Agregar** o **Modificar** para crear o editar el mapeo entre el número DID deseado y el anexo flotante o intervalo de ellos.
Reenviar todas las llamadas	Envía todas las llamadas a este anexo hacia el número especificado. Si el número es externo, incluya cualquier código de acceso que sea necesario.
Activar correo de voz	Se crea un buzón de correo de voz para este anexo. Cuando se realiza esta configuración, se necesita información del usuario.
Información del usuario La información del usuarios sólo se necesita si es necesario el servicio Discado por nombre de la contestadora automática o si se desea activar el correo de voz para el anexo flotante.	
Nombre	Nombre del usuario asociado con este anexo flotante. Aparece en el directorio y se usa para el servicio Discado por nombre de la contestadora automática.
Apellido	Apellido del usuario asociado con este anexo flotante. Aparece en el directorio y se usa para el servicio Discado por nombre de la contestadora automática.
ID de usuario	ID del usuario asociado con este anexo flotante. Esta ID del usuario se utiliza cuando se inicia sesión en las páginas web de Opciones de usuario de Cisco Unity Express para cambiar la configuración de correo de voz.

Configuración	Descripción
Contraseña	Contraseña del usuario asociado con este anexo flotante. Esta contraseña se utiliza cuando se inicia sesión en las páginas web de Opciones de usuario de Cisco Unity Express para cambiar la configuración de correo de voz. La contraseña se aplica sólo a la GUI de Unity Express de Cisco y al Protocolo de acceso a mensajes a través de internet (IMAP). Si es un teléfono SCCP, este campo también se aplica a la GUI de Unified Communications Manager Express (CME) de Cisco.
Borrar campos de usuarios	Elimine toda información de usuarios de este anexo flotante.

Movilidad de anexos

La función Movilidad de anexos (EM) permite entregar movilidad telefónica a los usuarios finales.

Un servicio de inicio de sesión de usuarios permite que los usuarios de teléfonos IP de Cisco se registren en un teléfono con EM activada donde pueden hacer y recibir llamadas usando su número de directorio personal y, opcionalmente, acceder a su buzón de correo de voz personal.

Para obtener información acerca de la función Movilidad de anexos y la configuración de cada ficha, consulte estas secciones:

- **Ejemplo de escenarios de implementación de movilidad de anexos**
- **Perfil de usuario con EM**
- **Perfil de teléfono con EM**

Visión general

Para configurar Movilidad de anexos para un sitio, debe realizar estos pasos:

- **Configuración general**. Es la configuración global que se aplica a todos los teléfonos con EM activada. Se pueden configurar hasta 3 horas de cierre de sesión automáticas. A la hora especificada, todas las sesiones de EM en los teléfonos con EM activada cierran su sesión en forma automática. También

puede especificar si la historia que el usuario de EM llamada se borra al cerrar la sesión. Consulte **Configuración general, página 350**.

- **Crear perfiles de usuarios con EM**. El perfil del usuario con EM define las asignaciones de botones y la configuración de discado rápido que verá el usuario con EN cuando inicie sesión en un teléfono con EM activada. Todos los usuarios con EM deben tener una perfil. Consulte **Perfil de usuario con EM, página 348**.

  Crear perfiles de teléfonos con EM. El perfil del teléfono con EM define las asignaciones de botones y la configuración de discado rápido de un teléfono con EN cuando no hay usuarios con EM que hayan iniciado sesión en el teléfono. Múltiples teléfonos pueden asociarse con el mismo perfil de teléfono. Consulte **Perfil de teléfono con EM, página 349**. El perfil de teléfono de CCA también se conoce como Perfil de cierre de sesión en IOS de Cisco.

- **Activación de teléfonos IP seleccionados para el servicio con EM**. Un teléfono se activa para la función Movilidad de anexos cuando está asociado a un perfil de teléfono. **Cómo activar EM en un teléfono, página 349**.

Ejemplo de escenarios de implementación de movilidad de anexos

Esta sección describe algunos escenarios comunes de implementación de movilidad de anexos y una visión general de los pasos de configuración para cadaa uno.

Escenario 1: Empleados móviles comparten teléfonos con EM activada

En este escenario, un conjunto de teléfonos IP se activan para el servicio con EM. Múltiples empleados (por ejemplo, vendedores) comparten estos teléfonos con EM activada cuando están en el sitio, en vez de tener teléfonos de escritorio personales. Cada uno de los empleados móviles tiene un buzón de correo personal y sus propias asignaciones de botones y de discado rápido cuando inician sesión en un teléfono con EM activada.

En este tipo de implementación, será necesario:

1. Crear un perfil de teléfono con EM que especifique las asignaciones de botones y discado directo por defecto que tendrá el teléfono cuando nadie haya iniciado sesión en él. Típicamente, este es un perfil muy simple con permisos de llamadas restringidos. Consulte **Perfil de teléfono con EM, página 349**.
2. Activar el servicio de EM para cada uno de los teléfonos en el conjunto común asociándolo con un perfil de teléfono. Consulte **Cómo activar EM en un teléfono, página 349**.

3. Crear un perfil de usuario de EM para cada empleado móvil. Este perfil tendrá extensiones personales del empleado y de marcado rápido. En cada perfil de usuario EM, habilitar y asignar un buzón personal de extensión principal del usuario. Consulte **Perfil de usuario con EM, página 348**.

Escenario 2: Los empleados móviles comparten teléfonos comunes cuando están en el sitio, pero tienen su propio teléfono IP en otra ubicación.

En este escenario, un conjunto de teléfonos comunes en un sitio se activan para el servicio con EM. Los empleados móviles comparten estos teléfonos cuando están en el sitio, pero también tienen un teléfono IP primario en otra ubicación. Cuando inician sesión en un teléfono con EM activada, sus anexos normales y compartidos y sus discados directos son los mismos que en su teléfono IP primario. Pueden acceder a su buzón de correo personal desde un teléfono con EM activada, además de su teléfono primario.

En este tipo de implementación, será necesario:

1. Crear un perfil de teléfono con EM que especifique las asignaciones de botones y discado directo por defecto que tendrá el teléfono cuando nadie haya iniciado sesión en él. Típicamente, este es un perfil muy simple con permisos de llamadas restringidos. **Perfil de teléfono con EM, página 349**.
2. Activar el servicio de EM para cada uno de los teléfonos en el conjunto común asociándolo con el perfil de teléfono con EM que se creó. **Cómo activar EM en un teléfono, página 349**.
3. Crear un perfil de usuario con EM para cada empleado móvil con las asignaciones de botones y discados directos deseados. Consulte **Perfil de usuario con EM, página 348**.

   Para que el usuario con EM use el mismo número de teléfono en un teléfono con EM activada y en su teléfono IP privado, debe usarse una línea compartida para el número primario. Para acceder al mismo buzón de correo de voz, debe estar activada la línea compartida con un buzón de correo compartido personal.

   Para que el usuario con EM use el mismo número de teléfono y buzón de correo de voz en un teléfono con EM activada y también su teléfono IP privado, debe privisionarse una línea compartida como el número primero con la opción de buzón de voz activada.

Requisitos y limitaciones

Se aplican las siguientes limitaciones a la configuración de Movilidad de anexos usando CCA:

- Se necesita Unified CallManager Express (CME) de Cisco, versión 8.0 ó posterior.
- CCA admite sólo los tipos de línea normal y compartida en los perfiles de usuario y teléfono.
- El número máximo de usuarios con EM admitidos es igual tres (3) veces el número de licencias de licencias para la plataforma UC500 que tiene el cliente (3 turnos de trabajo).
- Si desea que un usuario EM tener también un teléfono, asigne el mismo número que el perfil de EM y el teléfono del usuario utilizando una línea compartida. Configure el buzón de voz para la línea compartida como buzón de voz (compartido) personal.
- Los usuarios de teléfonos existentes no pueden convertirse automáticamente en usuarios de movilidad de anexo y éstos no pueden convertirse automáticamente a los usuarios de teléfonos regulares. Se debe eliminar manualmente al usuario de la ficha usuarios y anexos y volver a crear el usuario creando un perfil de usuario en la ficha movilidad de anexos. El buzón de voz del usuario existente se eliminará.
- No se entregan teclas para el acceso directo a la función Movilidad de anexos en los teléfonos con EM. Los usuarios con EM deben ir al menú Servicios CME en su teléfono y seleccione el elemento del menú Movilidad de anexo para iniciar y cerrar sesión.
- Un perfil de usuario sólo puede estar activo en un teléfono a la vez. Cuando un usuario con EM que ya inició sesión en un teléfono inicia sesión en otro diferente usando el mismo perfil, automática se cierra su sesión en el primer teléfono.
- No se admite el bloqueo de llamadas fuera del horario de trabajo.

Perfil de usuario con EM

El perfil del usuario con EM define los botones y discados rápidos que verá el usuario con EN cuando inicie sesión en un teléfono con EM activada.

Si es necesario un buzón de correo personal para el usuario, se debe activarlo. Un ID de usuario, su contraseña, nombre y apellido son necesarios al crear un perfil de usuario con EM.

Para crear o editar un perfil de usuario con EM, siga estos pasos.

PASO 1 En la ficha Movilidad de anexos de la ventana Usuarios y teléfonos, seleccione la ficha Perfiles de usuarios.

PASO 2 Para crear un nuevo perfil de usuario con EM, haga clic en **Agregar**.

PASO 3 Para editar un perfil de usuario con EM existente, ubique al usuario en la lista de perfiles, haga clic en la fila para seleccionar ese perfil de usuario y haga clic en **Editar**.

PASO 4 Realice la configuración como se describe en **Agregar perfil de usuario de movilidad de anexo, página 351**.

PASO 5 Haga clic en **Aceptar**.

Perfil de teléfono con EM

El perfil del teléfono con EM define las asignaciones de botones y la configuración de discado rápido de un teléfono con EN cuando no hay usuarios con EM que hayan iniciado sesión en el teléfono. Múltiples teléfonos pueden asociarse con el mismo perfil de teléfono.

Para crear o editar un perfil de teléfono con EM, siga estos pasos.

PASO 1 En la ficha Movilidad de anexos de la ventana Usuarios y teléfonos, seleccione la ficha Perfiles de telefónos.

PASO 2 Para crear un nuevo perfil de teléfono con EM, haga clic en **Agregar**.

PASO 3 Para editar un perfil de teléfono con EM existente, ubique al teléfono en la lista de perfiles, haga clic en la fila para seleccionar ese perfil de teléfono y haga clic en **Editar**.

PASO 4 Realice la configuración como se describe en **Agregar perfil de Teléfono de movilidad de anexo, página 354**.

PASO 5 Haga clic en **Aceptar**.

Cómo activar EM en un teléfono

Para activar la función Movilidad de anexos en un teléfono, siga estos pasos.

PASO 1 En la ficha Anexos de usuario de la ventana Usuarios y teléfonos, haga clic en un teléfono de la lista y haga clic en **Editat** o en **Agregar** para agregar un nuevo teléfono.

PASO 2 En la sección Movilidad de anexos de la ventana Agregar o editar configuración de teléfonos, marque la opción **Activar movilidad de anexos**.

Cuan do se activa la función movilidad de anexos en un teléfono:

- Si es un teléfono nuevo, toda la información del usuario y sus asignaciones de línea se desactivan.
- Si un usuario está asociado con el teléfono, toda la información del usuario y sus asignaciones de botones y discados directos se borran y se eliminarán cuando se apliquen los cambios.
- Si un usuario asociado con el teléfono tiene un buzón de correo de voz personal, éste también se elimina cuando se aplica la configuración.

PASO 3 En la lista desplegable **Seleccionar perfil de teléfono**, seleccione el perfil de teléfono con EM que se asociará con este teléfono.

Cuando se selecciona un perfil de teléfono, el área de Información de usuario de la ventana se actualiza para mostrar la información del usuario que está configurada para ese perfil de teléfono.

PASO 4 Haga clic en **Aceptar**.

Configuración general

Realice la configuración de cierre de sesión global para todos los teléfonos con EM activada en su sitio como se describe a continuación, luego haga clic en **Aceptar**.

Configuración	Descripción
Cierre de sesión auomático	Configure hasta 3 horas de cierre de sesión automático, usando un formato de 24 horas. Esta configuración de cierre de sesión automático se aplica a todos los teléfonos con EM activada. A la hora especificada de cierre de sesión automático, todas las sesiones en los teléfonos con EM activada cierran su sesión en forma automática. Si una llamada está en curso en el momento de auto-cierre de sesión, la sesión del usuario se registra después de que termine la llamada.
Borrar historial de llamadas luego del cierre de sesión del usuario	Cuando se marca esta opción, se elimina el historial de llamadas del usuario con EM que ha iniciado su sesión cuando este usuario cierra su sesión o ésta se cierra en forma automática.

Agregar perfil de usuario de movilidad de anexo

Esta ventana aprece cuando se hace clic en **Agregar** o en **Editar** en la ficha Perfiles de usuarios en Movilidad de anexos de la ventana Usuarios y teléfonos. También se puede hacer doble clic en un perfil de usuario con EM existente para abrir esta ventana.

El perfil del usuario con EM define las asignaciones de botones y la configuración de discado rápido que verá el usuario con cuando inicie sesión en un teléfono con EM activada. Todos los usuarios con EM deben tener una perfil. También se puede seleccionar activar un buzón de correo personal para el usuario con EM.

Configure un perfil de usuario como se describe a continuación y luego haga clic en **Aceptar**.

Configuración	Descripción
Configuración de perfil	
ID de usuario **Contraseña**	*Obligatorio*. Escriba la ID y contraseña del usuario para iniciar sesión en los teléfonos con EM activada. Debido a que el usuario escribirá su ID y contraseña en el teclado del teléfono para iniciar sesión, ésta debe ser breve. La misma ID y contraseña de usuario también definen la credencial de inicio de sesión para acceder al GUI de CUE.
Nombre **Apellido**	*Obligatorio*. El nombre y apellido del usuario del perfil de EM también se incluyen en el directorio y se usan para el servicio de discado por nombre de la contestadora automática.
Límite de tiempo automático de cierre de sesión (minutos)	Escriba el número de minutos del tiempo desocupado que desea que transcurra antes de cerrar automáticamente la sesión del usuario del perfil.

Configuración	Descripción
Activar botón de privacidad	Cuando se marca la opción **Activar botón de privacidad**, se coloca un botón Privacidad en el teléfono. El botón de privacidad se usa en conjunto con la función Conference Barge (cBarge). IOS coloca el botón Privacidad en el teléfono automática de acuerdo con las siguientes normas: ▪ El botón Privacidad se asigna después de la aparición de la última línea o botón de funciones y no puede ser colocada entre botones de línea o funciones. Por ejemplo, si se está usando los botones 1 y 2, entonces el botón Privacidad se asigna al botón 3. Si se está usando los botones 1, 2 y 5, entonces el botón Privacidad se asigna al botón 6, aunque los botones 3 y 4 esté en desuso. ▪ Si no hay suficientes botones en el teléfono físico, el botón Privacidad no aparecerá en el teléfono.

Configuración	Descripción
Detalles	
Línea	Seleccione la ficha **Línea** para asignar botones a este perfil de usuarios con EM. ▪ Para agregar o eliminar líneas de anexos, especifique el número de anexos deseados en **Número de líneas de anexos**. Es posible agregar hasta 69 anexos. Para cada botón: ▪ Seleccione un **Tipo de botón**, ya sea **Normal** o **Compartido**. Consulte **Anexo normal, página 358** y **Anexo compartido, página 363** para obtener más información acerca de la configuración de opciones para estos tipos de botones. ▪ Especifique el número de anexo o seleccione uno compartido. ▪ Escriba una etiqueta descriptiva para el botón. Esta etiqueta aparecerá en el teléfono. ▪ *Opcional*. Marque la opción **Buzón** de correo para crear un buzón de correo para este anexo.
Discado rápido	Seleccione la ficha Línea para asignar discados directos a este perfil de usuario con EM. Para obtener más información, consulte **Discado rápido, página 339**.

Agregar perfil de Teléfono de movilidad de anexo

Esta ventana aprece cuando se hace clic en **Agregar** o en **Editar** en la ficha Perfiles de teléfono en Movilidad de anexos de la ventana Usuarios y teléfonos.

El perfil del teléfono con EM define los botones y discados rápidos que verá el usuario cuando no haya usuarios con EM usando el teléfono.

Configure un perfil del teléfono como se describe a continuación y luego haga clic en **Aceptar**.

Configuración	Descripción
Configuración de perfil	
ID de usuario **Contraseña**	*Opcional*. La ID y contraseña del usuario sólo se necesitan si hay un buzón de correo activado para este perfil de teléfono. La misma ID y contraseña de usuario también definen la credencial de inicio de sesión para acceder al GUI de CUE.
Nombre **Apellido**	*Opcional*. El nombre y apellido del usuario sólo se necesitan si hay un buzón de correo activado para este perfil de teléfono. Si se definen, el nombre y apellido del usuario del perfil de EM también se incluyen en el directorio y se usan para el servicio de discado por nombre de la contestadora automática.

Configuración	Descripción
Activar botón de privacidad	El botón de privacidad se usa en conjunto con la función Conference Barge (cBarge). IOS coloca el botón Privacidad en el teléfono automática de acuerdo con las siguientes normas: ▪ El botón Privacidad se asigna después de la aparición de la última línea o botón de funciones y no puede ser colocada entre botones de línea o funciones. Por ejemplo, si se está usando los botones 1 y 2, entonces el botón Privacidad se asigna al botón 3. Si se está usando los botones 1, 2 y 5, entonces el botón Privacidad se asigna al botón 6, aunque los botones 3 y 4 esté en desuso. ▪ Si no hay suficientes botones en el teléfono físico, el botón Privacidad no aparecerá en el teléfono. El botón Pivacidad del perfil del teléfono tambien puede verse en la ventana **Telefonía** > **Funciones de voz** > **Conference Barge** después que se ha asignado a un teléfono.

Configuración	Descripción
Detalles	
Línea	Seleccione la ficha Línea para configurar el número de líneas de anexos y asignar botones a este perfil de teléfonos con EM. ▪ Para agregar o eliminar líneas de anexos, especifique el número de anexos deseados en **Número de líneas de anexos**, y luego haga clic en **Aceptar**. Es posible agregar hasta 69 líneas de anexos. ▪ Para cada botón, seleccione un tipo de botón, escriba o seleccione un anexo para asigarlo y escriba una etiqueta descriptiva para el botón. Sólo se pueden agregar botones de teléfonos **Normal** y **Compartido**. Consulte **Anexo normal, página 358** y **Anexo compartido, página 363** para obtener más información acerca de la configuración de la sección de botones para estos tipos de botones.
Discado rápido	Seleccione la ficha Línea para asignar discados directos a este perfil de usuario de teléfonos. Para obtener más información, consulte **Discado rápido, página 339**.

Anexos analógicos

Los puertos indicados en la ficha Anexos analógicos son puertos FXS que se han configurado con el perfil **Teléfono o fax de área común** de la ventana **Configurar** > **Telefonía** > **Puertos y enlaces**>**Puertos FXS**. Estos dispositivos incluyen teléfonos análogos y máquinas de fax de legado.

Estas notas se aplican al configurar anexos análogos:

- En el campo **Anexo**, escriba un anexo único.
- Las funciones avanzadas, como correo de voz, desvío de llamadas, etc., no están disponibles en los teléfonos configurados como anexos analógicos.

- Para evitar que el usuario llame los números restringidos (bloqueados) configurados en el plan de numeración saliente, marque la casilla **Bloquear números restringidos**.
- La configuración **Permisos** especifica el tipo de llamadas salientes que pueden realizarse desde este teléfono. Para obtener más información, consulte **Permisos, página 361**.

Luego de realizar cambios en esta ventana, haga clic en **Guardar configuración** para aplicar la configuración.

Configuración de asignaciones de botones de teléfonos

Para conocer información sobre los tipos de botones que pueden configurarse en el teléfono e información detallada acerca del botón <#> y su configuración (donde <#> representa el número del botón), consulte las siguientes secciones:

- **Anexo normal, página 358**
- **Anexo compartido, página 363**
- **Configuración de un buzón (compartido) personal o GDM para un Anexo compartido, página 365**
- **Monitorear, página 366**
- **Observar, página 366**
- **Línea CO, página 367**
- **Anexo de sobrecapa, página 368**
- **Intercom, página 369**
- **Intercomunicador discable, página 370**
- **Intercomunicador de susurros, página 373**
- **Líneas octales, página 375**

Anexo normal

Cuando se configura un botón de teléfono como un anexo normal, se asigna un solo anexo al botón.

Para configurar la sección del **Botón<#>** para un botón de anexo normal, siga estos pasos.

PASO 1 Seleccione **Configurar** > **Telefonía** > **Usuarios y anexos**>**Usuarios y teléfonos** y seleccione la ficha Anexos de usuarios.

PASO 2 Haga clic en un teléfono de la lista para seleccionarlo, y haga clic en el botón **Editar** para mostrar los detalles de su configuración.

PASO 3 Seleccione la ficha **Asignaciones de botones**tab.

PASO 4 Seleccione un número de botón.

PASO 5 En la sección del **Botón<#>** , realice la configuración para el anexo como se describe a continuación.

Campo	Descripción
Tipo de botón	Usando el menú desplegable, confígurelo como **Normal**.
Ficha Parámetros	
Anexo	Escriba el número del anexo desado para esta línea.
Etiqueta del botón	Escriba la etiqueta deseada para este botón.
Descripción	Especifique una descripción para este teléfono. Este descripción se muestra en la esquina superior derecha del teléfono. Los carácteres válidos en este son carácteres alfanuméricos (A-Z, a-z, 0-9, espacios, punto(.), guión bajo (_), y signo menos (-). Por ejemplo, su cliente puede necesitar que se muestre el número de teléfono completo discado directo entrante (DID) en los teléfonos. Se puede editar este campo de descripción para que muestre el número DID, por ejemplo, 555 555-5555.

Campo	Descripción
Línea dual o Línea Octal	Tipo de línea, ya sea dual u octal. Esta selección se aplica sólo a los tipos de botones Normales y Compartidos. El valor por defecto es Línea octal, si el teléfono admite esta función. Un número de directorio de línea octal admite hasta ocho llamadas activas, tanto entrantes como salientes, en un solo botón telefónico. La línea octal no está disponible para teléfonos que no admitan esta función. Las líneas octales sólo están disponibles si el UC500 está ejecutando la versión 12.4(20)T ó posterior de IOS de Cisco y la versión del paquete de software del UC500 de Cisco es 7.0(2) ó posterior. Para obtener más información, consulte **Líneas octales, página 375**. Se necesita un anexo compartido de línea octal para activar la función Conference Barge (cBarge). Consulte **Conference Barge, página 422**.
Activar correo de voz	Haga clic para activarlo (marcado) o desactivarlo (sin marca). Cuando se marca la opción Buzón de correo para una línea normal, se crea un buzón de correo personal para este anexo. Sólo puede crearse un buzón de correo personal por usuario. El buzón de correo y sus contenidos no se eliminan cuando se vuelve a asociar el buzón de correo con un anexo diferente.
Bloquear números restringidos	Para evitar que el usuario llame los números restringidos (bloqueados) configurados en el plan de numeración saliente, marque la casilla **Bloquear números restringidos**.

Campo	Descripción
Permisos	Esta configuración especifica el tipo de llamadas salientes que pueden realizarse desde este teléfono. Los niveles de permisos se definen en la ficha del plan de numeración saliente (**Configurar** > **Telefonía** > **Plan de numeración** > **Saliente**, y seleccione la ficha Gestión de llamadas salientes). Realice una de las siguientes acciones: ▪ **Sin restricciones**. Puede realizar llamadas salientes al PSTN sin ninguna restricción. ▪ **Interno**. Puede realizar llamadas salientes sólo al discar números internos y de emergencia. Con restricciones para realizar todas las demás llamadas. ▪ **Local**. Puede realizar llamadas salientes sólo al discar números locales, internos y de emergencia. Con restricciones para realizar llamadas locales más internacionales o de larga distancia nacional. ▪ **Local plus**. Puede realizar llamadas salientes discando números locales, internos y de emergencia, más números locales adicionales según se defina en el plan de numeración saliente. ▪ **Nacional**. Puede realizar llamadas salientes sólo al discar números nacionales de larga distancia, locales, internos y de emergencia. Con restricciones para realizar llamadas nacionales más números y llamadas internacionales. ▪ **National plus**. Puede realizar llamadas salientes sólo discando números nacionales de larga distancia, locales, internos y de emergencia, más números locales adicionales según se defina en el plan de numeración saliente. Con restricciones para realizar llamadas internacionales. ▪ **Internacional**. Puede realizar llamadas salientes al discar números locales, internos, de larga distancia nacional, internacionales y de emergencia.

Campo	Descripción
Desvío ocupado	Transfiere las llamadas a este anexo cuando esta línea está ocupada. Haga clic en el campo e indique un anexo para cambiar la configuración. Si la opción de correo de voz está activada y Desvío de llamadas ocupado está desactivada, Desvío de llamadas de disponibilidad establecido en el número de extensión de correo de voz.
Desvío sin respuesta	Transfiere las llamadas entrantes a este anexo si no hay respuesta. Haga clic en el campo e indique un anexo para cambiar la configuración. Si la opción de correo de voz está activada, pero el Desvío de llamadas sin contestación está desactivada, Desvío de llamadas sin contestación se establece en el número de extensión de correo de voz.
Límite de tiempo de CFNA, segundos	Número de segundos antes que las llamadas no contestadas se transfieran al destino de Desvío sin respuesta. Por defecto es de 20 segundos. **IMPORTANTE** Si este anexo es un miembro de un Grupo de envío de llamadas, el valor de **Límite de tiempo de CFNA** que se configuró debe ser mayor que el valor del Límite de tiempo configurado para el Grupo de envío de llamadas. Por ejemplo, si el valor del Límite de tiempo para el Grupo de envío de llamadas al que pertenece el anexo es de 10 segundos, configure el límite de tiempo de CFNA para dicho anexo a, al menos, 11 segundos. Como alternativa, se puede bajar el valor del límite de tiempo para el Grupo de envío de llamadas. Consulte **Llamar a grupos de envío, página 402**.
Número PSTN	El campo de sólo lectura que muestra el número PSTN que está mapeado hasta este anexo en el plan de numeración entrante, si está configurado. Para mapear números de DID hacia anexos internos, seleccione **Configurar** > **Telefonía** > **Plan de numeración** > **Entrante**, seleccione la ficha **Discado directo** y realice la configuración en **Discado directo a anexos internos**.

Campo	Descripción
Ficha Alerta de llamada en espera	
La función Alerta de llamada en espera permite configurar un tono de alerta audible y repetitivo para notificar al usuario cuando una llamada se pone en espera en un teléfono IP de Cisco.	
Alerta de llamada en espera	Seleccione una de las siguientes configuraciones para especificar cuándo se reproducirán los tonos de alerta de llamada en espera. ▪ **Ninguno** Las alertas están desactivadas. Ésta es la configuración predeterminada. ▪ **Cuando esté desocupado**. Las alertas se reproducen sólo cuando el teléfono está desocupado. ▪ **Cuando esté desocupado u ocupado**. Las alertas se reproducen sólo cuando el teléfono está ocupado o desocupado. ▪ **Cuando esté desocupado en alerta compartida**. Las alertas se reproducen sólo cuando el anexo está desocupado. Las alertas se reproducen en todos los teléfonos que comparten este anexo.
Límite de tiempo	Número de segundos entre notificaciones de alertas audibles. Especifique un número entre 15 y 300. Por ejemplo, si este valor se fija a 25 segundos, el tono de alerta de llamada en espera se reproduce una vez cada 25 segundos.

PASO 6 Haga clic en **Aceptar**.

Anexo compartido

Se puede configurar un anexo compartido y agregar un botón para el anexo compartido para múltiples teléfonos para que las llamadas entrantes a ese anexo hagan sonar todos los teléfonos con un botón para el anexo compartido.

Para obtener información acerca de la creación de buzones de correo de voz para los anexos compartidos, consulte **Configuración de un buzón (compartido) personal o GDM para un Anexo compartido, página 365**.

Para configurar un anexo compartido, siga estos pasos.

PASO 1 Configure los teléfonos y usuarios, según se describe en **Cómo agregar un teléfono, página 330**.

PASO 2 Seleccione **Configurar** > **Telefonía** > **Usuarios y anexos**> **Usuarios y teléfonos** para abrir la ventana Usuarios y teléfonos y seleccione la ficha Anexos de usuarios.

PASO 3 Haga clic en un teléfono para seleccionarlo, y haga clic en el botón **Editar** de la parte inferior de la ventana para visualizar sus detalles.

PASO 4 Haga clic en la ficha **Asignaciones de botones**tab.

PASO 5 Seleccione un número de botón de la tabla y configure su tipo como **Compartir**.

PASO 6 En el campo **Anexo** para ese botón del teléfono, especifique o seleccione el anexo que utilizará la línea compartida.

- Para crear un nuevo anexo compartido, escriba un número de anexo único para usarlo para el anexo compartido.
- Para colocar un anexo compartido existente en el botón de teléfono seleccionado, seleccione un anexo de la lista desplegable.
- Si seleccionó el botón 1 en el teléfono para el anexo compartido, sólo los anexos compartidos del botón 1 de los otros teléfonos se indican en la lista desplegable.
- Si selecionó un botón distinto al botón 1, sólo los anexos compartidos que no estén en el botón 1 aparecen en la lista desplegable.

PASO 7 Si es un nuevo anexo compartido, configure la sección del **Botón<#>** para la línea compartida, como se describe en la sección **Anexo normal, página 358**.

Los buzones de correo de voz se tratan en forma diferente para los anexos compartidos. Para obtener más información, consulte **Configuración de un buzón (compartido) personal o GDM para un Anexo compartido, página 365**.

PASO 8 En el campo **Nombre compartido**, especifique el nombre que se usará para este anexo compartido. Es necesario un nombre si el anexo compartido está en un botón no primario.

NOTA El campo**Nombre compartido** se desactiva si el anexo compartido se coloca en el botón 1 del teléfono. Para los anexos compartidos colocados en el botón 1, la información del usuario se carga previamente a partir del usuario para el que se creó inicialmente el anexo compartido (excepto su ID y contraseña de usuario, la que debe ser única para cada teléfono).

PASO 9 Haga clic en **Aceptar** cuando termine.

PASO 10 Realice llamadas al anexo compartido para verificar que los anexos están compartidos en los teléfono, según lo esperado.

Configuración de un buzón (compartido) personal o GDM para un Anexo compartido

Cuando se activa el correo de voz para un anexo compartido, el tipo de buzón de correo que se crea es, por defecto, diferente entre los anexos que se colocan en el botón 1 de un teléfono que para los otros botones del teléfono:

- Si se marca **Activar correo de voz** para un anexo compartido en el botón 1 de un teléfono, se crea un buzón (compartido) personal por defecto. Esta funcionalidad está pensada para casos en que un solo usuario tiene múltiples teléfonos pero desea un solo buzón de correo personal al que pueda acceder desde todos sus teléfonos.
  Si, por algún motivo, el usuario con múltiples teléfonos no desea usar el botón 1 para ello, es posible crear el anexo compartido en un botón diferente, luego ir a la ficha Buzones de correo de la ventana Correo de voz, cambiar Buzón de correo GDM a un buzón de correo (compartido persona) y seleccionar la ID del usuario deseado de la lista desplegable. Sólo usuarios con este anexo compartido que no tengan actualmente un buzón de voz Personal aparecen en la lista. Una vez que se cambie el tipo de buzón de correo a Personal y se seleccione un usuario, CCA elimina el buzón de correo GSM y crea un buzón de correo (compartido) personal para el anexo compartido usando la ID del usuario especificada.

  En forma alternativa, primero se podría definir un anexo normal para el usuario y asignarle un buzón de correo personal, luego, volver a definir el mismo anexo como anexo compartido usando el mismo número de anexo para activar el buzón de correo de voz. CCA conservará el buzón de correo personal y volverá a asociarlo con el anexo compartido.
- Si se marca **Activar correo de voz** para un anexo compartido en cualquier otro botón de un teléfono, se crea un buzón GDM (buzón grupal) por defecto. Al asignar un GDM a un anexo compartido en un teléfono, el usuario debe tener también un buzón de correo personal asignado para acceder al GDM usando su propio PIN de correo de voz personal.

  Cuando se agrega el anexo compartido a otros teléfonos, asegúrese de activar el buzón de correo para el anexo si desea que el usuario pueda acceder al buzón de correo GDM.

Monitorear

Un botón Monitor sólo monitorea el anexo especificado.

El estado de la línea indica si la línea está inactiva o en uso. Un recepcionista puede utilizar los botones de monitoreo para controlar el estado en uso de los anexos telefónicos.

Para configurar un botón Monitor, siga estos pasos:

PASO 1 Seleccione **Configurar** > **Telefonía** > **Usuarios y anexos>Usuarios y teléfonos** y seleccione la ficha Anexos de usuarios.

PASO 2 Haga clic en un teléfono de la lista para seleccionarlo, y haga clic en el botón **Editar** para mostrar los detalles de su configuración.

PASO 3 Seleccione la ficha **Asignaciones de botones**tab.

PASO 4 Seleccione un número de botón y configure su **Tipo** como **Monitor**.

PASO 5 En el ára del **Botón <#>** para este botón, seleccione el anexo que va a monitorearse de la lista desplegable. Los anexos de Parqueo de llamadas se incluyen en la lista de anexos que pueden monitorearse.

La etiqueta del anexo monitoreado se inserta automáticamente en el campo Etiqueta para el botón Monitorear.

PASO 6 Haga clic en **Aceptar**.

Observar

Un botón Observar permite que el usuario observe todas las líneas del teléfono con el anexo especificado.

El indicador del estado de línea en el botón Observar se enciende de color rojo cuando cualquier línea está en uso, fuera de servicio o en modo No molestar.

El usuario del teléfono puede presionar el botón Observar para discar rápidamente el anexo observado. Otras llamadas no pueden hacerse ni recibirse utilizando un botón de línea que esté en modo observar. Las llamadas entrantes en un botón de línea que esté en modo observar no campanillean ni muestran la ID de quien llama ni la ID de quien llama en espera.

Para configurar un botón de observación, siga estos pasos:

PASO 1 Seleccione **Configurar** > **Telefonía** > **Usuarios y anexos>Usuarios y teléfonos** y seleccione la ficha Anexos de usuarios.

PASO 2 Haga clic en un teléfono de la lista para seleccionarlo, y haga clic en el botón **Editar** para mostrar los detalles de su configuración.

PASO 3 Seleccione la ficha **Asignaciones de botones**tab.

PASO 4 Seleccione un número de botón y configure su **Tipo** como **Observación**.

PASO 5 En el ára del **Botón <#>** para este botón, seleccione el anexo que va a observarse de la lista desplegable.

La etiqueta del anexo observado se inserta automáticamente en el campo Etiqueta para el botón Observar.

PASO 6 Haga clic en **Aceptar**.

Línea CO

Seleccione Línea CO si desea asignar una línea de la Oficina central (línea de enlace directo) a este botón. No se puede asignar un buzón de voz a un botón de línea CO.

Para configurar un botón de línea CO, siga estos pasos:

PASO 1 Seleccione **Configurar** > **Telefonía** > **Usuarios y anexos>Usuarios y teléfonos** y seleccione la ficha Anexos de usuarios.

PASO 2 Haga clic en un teléfono de la lista para seleccionarlo, y haga clic en el botón **Editar** para mostrar los detalles de su configuración.

PASO 3 Seleccione la ficha **Asignaciones de botones**tab.

PASO 4 Seleccione un número de botón.

PASO 5 En el menú desplegable **Tipo** para el botón seleccionado, seleccione **Línea CO**, por ejemplo, **CO 1 (0/1/0)**.

Estos corresponden a las líneas de enlace PSTN directo conectadas a los puertos FXO. Edite la **Etiqueta** según sea necesario para identificar la línea CO.

PASO 6 En el ára del **Botón <#>** para este botón, seleccione la línea de enlace que va a usarse para la línea CO de la lista desplegable.

PASO 7 Haga clic en **Aceptar**.

Anexo de sobrecapa

Un anexo de Sobrecapa normal permite que múltiples líneas (hasta 25) compartan un solo botón en un teléfono con múltiples botones. Los anexos de sobrecapa necesitan, al menos, dos anexos normales, compartidos o de línea CO.

CCA también admite la configuración Sobrecapa en una Línea CO (Oficina central). Esta configuración permite que una Línea CO comparta un botón con un anexo regular. El usuario puede contestar llamadas en esa Línea CO y ver el estado de la línea, pero puede hacer y recibir llamadas usando el anexo regular. Esta funcionalidad es más útil en los teléfonos con un número limitado de botones.

NOTA Las líneas octales no admiten sobrecapas. Esto significa que los anexos que se configuran para funciones como Conferencias o Conference Barge (cBarge) no puede tener sobrecapas.

Para configurar un botón de sobrecapas, siga estos pasos:

PASO 1 Seleccione **Configurar** > **Telefonía** > **Usuarios y anexos>Usuarios y teléfonos** y seleccione la ficha Anexos de usuarios.

PASO 2 Haga clic en un teléfono de la lista para seleccionarlo, y haga clic en el botón **Editar** para mostrar los detalles de su configuración.

PASO 3 Seleccione la ficha **Asignaciones de botones**tab.

PASO 4 Seleccione un número de botón y configure su **Tipo** como **Sobrecapa**.

PASO 5 En el ára del **Botón <#>** para este botón, seleccione el anexo que va a usarse para la sobrecapa de la lista desplegable.

PASO 6 En el árae **Botón<#>**, realice esta configuración.

a. Seleccione si se activa o desactiva la espera de llamadas para este anexo de sobrecapa. Cuando se marca la opción **Activar espera de llamadas**, se activa esta función en el anexo de sobrecapas.

   Con la espera de llamadas activada, si el anexo de sobrecapa está en uso y llega una segunda llamada al anexo de sobrecapa, se reproduce el tono de espera de llamada y la llamada aparece en la pantalla del teléfono IP.

b. Use los botones **Agregar**, **Eliminar**, **Seleccionar todo** y **Seleccionar ninguno** para desplazar los anexos compartidos desde la lista Anexos disponibles

hasta la lista Anexos seleccionados.

Se debe selecconar al menos dos (2) anexos para el botón Sobrecapa. Los anexos normales, compartidos y de linea CO aparece en la lista de Anexos disponibles.

c. Use las flechas **Hacia arriba** y **Hacia abajo** para volver a ordenar los anexos de la lista Anexos seleccionados.

d. *Opcional*. En el campo **Etiqueta de botón sobrecapa**, escriba un nombre descriptivo para que este anexo lo muestre en el teléfono.

Por defecto, la etiqueta para el primer número de anexos de la lista Seleccionados se utiliza para la etiqueta del botón de sobrecapa. Cuando se edita la etiqueta del botón de sobrecapa, la etiqueta para el primer número de anexo también se cambia.

PASO 7 Haga clic en **Aceptar**.

Intercom

Un botón de intercomunicador es un botón único que se presiona para hablar entre dos teléfonos IP.

- Pueden configurarse múltiples intercomunicadores en un teléfono.
- No se puede configurar el botón 1 como un intercomunicador.

Para configurar un botón de intercomunicador, siga estos pasos:

PASO 1 Seleccione **Configurar** > **Telefonía** > **Usuarios y anexos>Usuarios y teléfonos** y seleccione la ficha Anexos de usuarios.

PASO 2 Haga clic en un teléfono de la lista para seleccionarlo, y haga clic en el botón **Editar** para mostrar los detalles de su configuración.

PASO 3 Seleccione la ficha **Asignaciones de botones**tab.

PASO 4 Seleccione un número de botón y configure su **Tipo** como **Intercomunicador**.

PASO 5 En el área **Botón<#>** para este botón, realice esta configuración.

a. En la lista desplegable **Usuario objetivo del botón de intercomunicador**, seleccione un usuario objetivo. El botón de intercomunicador se coloca en el teléfono del usuario.

b. En la lista desplegable **Número de botón del intercomunicador objetivo**, seleccione un botón disponible en el teléfono del usuario objetivo que se usará para el intercomunicador.

c. En el campo **Etiqueta para el usuario objetivo**, especifique el texto que desea mostrar en el escritorio del teléfono del usuario objetico al lado de este botón Intercomunicador.

   Cuando se presiona el botón Intercomunicador en el teléfono de este usuario, se muestra el texto de etiqueta en el campo Desde: de la información sobre la llamada que aparecen en el teléfono del usuario de destino.

d. En el campo **Etiqueta para el usuario actual**, especifique el texto que desea mostrar en el escritorio del teléfono de este usuario para este botón de Detalles de Intercomunicador.

   Cuando se presiona el botón Intercomunicador, se muestra este texto en el campo A: de la información llamando al teléfono del usuario.

PASO 6 Seleccione si se activará o desactivará Silencio para este intercomunicador.

Cuando se activa (marca) la opción **Con silenciador**, el receptor del intercomunicador debe desactivar el silenciador presionando el botón Silenciador de su teléfono o levante el auricular para responder al intercomunicador.

Cuando se desactiva (desmarca) la opción **Con silenciador**, ambas partes se escuchan entre sí cuando se conecta la llamada.

PASO 7 Haga clic en **Aceptar**.

Intercomunicador discable

Para obtener mayor información sobre los Intercomunicadores discables, consulte estas secciones:

- **Descripción de función, página 371**
- **Teléfonos no admitidos, página 372**
- **Pasos de configuración, página 372**

Descripción de función

Botón del intercomunicador que permite que un usuario se comunique con otro teléfono del sistema que también tenga un botón de intercomunicador discable al presionar el botón del intercomunicador y discar el anexo por medio del intercomunicador.

A diferencia de los Intercomunicadores de susurros y los Intercomunicadores normales, que siempre están configurados entre dos teléfonos específicos, los usuarios de teléfonos puede intercomunicarse con otros teléfonos presionando el botón Intercomunicador de su teléfono y discando un anexo de Intercomunicador discable.

Los Intercomunicadores discables los usan los operadores o personal administrativo que proporcionan soporte para muchos empleados, a diferencia de los asistentes administrativos que, por lo general, son responsables de uno o dos personas y tienen botones de intercomunicación específicos para cada persona en su teléfono. When this feature is used, a Dialable Intercom button is usually configured on every user's phone.

Sólo puede configurarse in botón de intercomunicador discable por teléfono.

CCA no permite que se configuren Intercomunicadores discables en el botón 1 de un teléfono.

En forma opcional, se puede configurar el Intercomunicador discable con o sin silencio.

- Cuando está activado **Silencio** para el intercomunicador, el teléfono al que se llama contesta automáticamente en un modo de parlante con el Silencio activado. El teléfono hace sonar un "bip" cuando la llamada por intercomunicador se contesta automáticamete para alertar al receptor acerca de la llamada entrante por el intercomunicador.

  Para responder a la llamada por intercomunicador y activar el audio bidireccional, el receptor desactiva la función Silencio presionando el botón Silencio de su teléfono o, en algunos teléfonos, levantando el auricular.

- Cuando se desactiva **Silencio**, tanto quien llama como el receptor se escuchan entre sí de inmediato cuando se conecta la llamada por el intercomunicador.

  El beneficio de desactivar Silencio es que el receptor de la llamada por intercomunicador puede hablar sin tener que primero desactivar la función Silencio. Sin embargo, sonidos o conversaciones cercanas pueden escucharse tan pronto como se conecta la llamada por el intercomunicador.

Teléfonos no admitidos

Los Intercomunicadores discables no se admiten en estos teléfonos:

- Teléfonos análogos
- ATA

Pasos de configuración

Para configurar el botón Intercomunicador discable, siga estos pasos:

PASO 1 Seleccione **Configurar** > **Telefonía** > **Usuarios y anexos>Usuarios y teléfonos** y seleccione la ficha Anexos de usuarios.

PASO 2 Haga clic en un teléfono de la lista para seleccionarlo, y haga clic en el botón **Editar** para mostrar los detalles de su configuración.

PASO 3 Seleccione la ficha **Asignaciones de botones**tab.

PASO 4 En la lista de botones, haga clic en el número del botón que desee usar para el Intercomunicador discable.

Sólo puede configurarse in botón de intercomunicador discable por teléfono.

PASO 5 En el menú desplegable **Tipo**, seleccione **Intercomunicador discables**.

PASO 6 En el área de opciones **Intercomunicador discabl**a la derecha, realice esta configuración.

a. Seleccone un anexo del menú desplegable **Dígitos de discado**. Éste es el anexo que marcan los usuarios del sistema para intercomunicarse con este teléfono. Se indican todos los anexos normales configurados en el teléfono.

b. Seleccione si se activará o desactivará **Silencio** para las llamadas por intercomunicadores.

   Cuando se activa **Silencio**, el teléfono que recibe la llamada la contesta automáticamente en modo de parlante con el Silencio activado y el receptor de la llamada debe desactivar el botón Silencio para poder hablar. Cuando se desactiva **Silencio**, ambos particpantes de la llamada por intercomunicador se escuchan entre sí de inmediato.

PASO 7 *Opcional*. En la columna **Etiqueta** de la lista de botones, edite la etiqueta para el botón Intercomunicador discable que se indica en el teléfono. La etiqueta por defecto es Intercomunicador discable<*Anxo*>.

PASO 8 Haga clic en **Aceptar**.

Intercomunicador de susurros

El Intercomunicador de susurros permite hacer una llamada por el intercomunicador a un anexo ocupado. Quien llama sólo puede ser escuchado por quien recibe la llamada. Para obtener más información, consulte estas secciones:

- **Descripción de función, página 373**
- **Requisitos y limitaciones, página 373**
- **Teléfonos no admitidos, página 374**
- **Procedimientos, página 374**

Descripción de función

Para hacer una llamada por Intercomunicador de susurros, el usuario del teléfono presiona el botón Intercomunicador de susurros en su teléfono.

- El teléfono recibe una llamada de intercomunicación Susurro muestra la extensión y el nombre del partido que inició la intercomunicación. Un tono juega antes de la fiesta llamada oye la voz de la persona que llama. El botón Intercomunicador de susurro se pone de color Ámbar para indicar audio unidireccional.
- Si el receptor de la llamada por Intercomunicador de susurros desea hablar al usuario que hizo la llamada, presiona el botón Intercomunicador de susurros en su teléfono, el que se pondrá de color verde para indicar audio bidireccional.
- Cuando el receptor de la llamada por Intercomunicador de susurros presione el botón Intercomunicador de susurros para hablar, la llamada activa de su teléfono se pone en espera en forma automática.

Para terminar una llamada por Intercomunicador de susurros, el usuario presiona la tecla **Terminar llamada**.

Requisitos y limitaciones

Los siguientes requisitos y limitaciones se aplican a los Intercomunicadores de susurros configurados usando CCA:

- El Intercomunicador de susurros necesita Cisco Unified CME 7.1 ó posterior y SCCP 12.0 ó posterior en los teléfonos IP.

- El Intercomunicador de susurros necesita CIPC 7.x ó posterior en los teléfonos CIPC (Cisco IP Communicator).
- Un botón Intercomunicador de susurros sólo puede hacer llamadas a otros Intercomunicadores de susurros.
- Sólo se permite una llamada por intercomunicadores (ya sea entrante o saliente) a la vez en un teléfono.

Teléfonos no admitidos

Los Intercomunicadores de susurros sólo están disponibles en los teléfonos que admiten líneas octales. Los Intercomunicadores de susurros no se admiten en estos teléfonos:

- Teléfonos FXS análogos
- ATA
- Teléfonos IP Modelo 7931 de Cisco con versiones de firmware anteriores a 8.5(3)
- Teléfonos IP Modelo 39xx de Cisco
- Teléfonos IP Modelo CP-521 de Cisco
- Teléfonos IP series SPA500 y SPA300 de Cisco
- Teléfonos IP Modelos 7902, 7905, 7906, 7910, 7911, y 7912 de Cisco
- Teléfonos IP Modelos 7940 y 7960 de Cisco

Procedimientos

Para configurar un botón de Intercomunicadores de susurro, siga estos pasos:

PASO 1 Seleccione **Configurar** > **Telefonía** > **Usuarios y anexos>Usuarios y teléfonos** y seleccione la ficha Anexos de usuarios.

PASO 2 Haga clic en un teléfono de la lista para seleccionarlo, y haga clic en el botón **Editar** para mostrar los detalles de su configuración.

PASO 3 Seleccione la ficha **Asignaciones de botones**tab.

PASO 4 Seleccione un número de botón y configure su **Tipo** como **Intercomunicador de susurros**.

PASO 5 En el área **Botón<#>** para este botón, realice esta configuración.

a. En la lista desplegable **Usuario objetivo del botón de intercomunicador**, seleccione un usuario objetivo. El botón de Susurro Intercomunicador se coloca en el teléfono del usuario.

b. En la lista desplegable **Número de botón del intercomunicador de susurros**, seleccione un botón disponible en el teléfono del usuario objetivo que se usará para el intercomunicador de susurros.

c. En el campo **Etiqueta para el usuario objetivo**, especifique el texto que desea mostrar en el escritorio del teléfono del usuario objetico al lado de este botón Intercomunicador de susurros.

   Cuando se presiona el botón Intercomunicador de susurros en el teléfono de este usuario, se muestra el siguiente texto en el campo Desde: de la información sobre la llamada que aparecen en el teléfono del usuario de destino.

d. En el campo **Etiqueta para el usuario actual**, especifique el texto que desea mostrar en el escritorio del teléfono de este usuario para este botón de Detalles de Intercomunicador de susurros.

   Cuando se presiona el botón Intercomunicador de susurros, se muestra este texto en el campo A: de la información llamando al teléfono del usuario.

PASO 6 Haga clic en **Aceptar**.

Líneas octales

Un número de directorio de línea octal admite hasta ocho llamadas activas, tanto entrantes como salientes, en un solo botón telefónico:

- A diferencia de un número de directorio de línea dual, el que se comparte exclusivamente entre teléfonos (después de contestar una llamada, esa llamada utiliza ambos canales del número del directorio de línea dual), un número de directorio de línea octal puede dividir sus canales entre otros teléfonos que compartan el número del directorio.
- A todos los teléfonos se les permite iniciar o recibir llamadas en los canales inactivos del número de directorio de la línea octal compartida. El número de directorio de la línea octal puede administrar múltiples llamadas. Múltiples llamadas entrantes a un número de directorio de línea octal suenan en forma simultánea.

- Después que un teléfono responde una llamada, el campanilleo se detiene y el tono de espera de llamadas se reproduce para las otras llamadas entrantes.
- Cuando los teléfonos compartes un número de directorio de línea octal, las llamadas entrantes suenan en teléfonos sin llamadas activas y estos teléfonos pueden contestar cualquiera de las llamadas que campanilleen. Los teléfonos con una llamada activa escuchan el tono de espera de llamadas.
- Despues que una llamada conectada en un número de directorio de línea octal se pone en espera, cualquier teléfono que comparta este número del directorio puede tomar la llamada en espera. Si un usuario telefónico está en el proceso de iniciar la transferencia de llamadas o crear una conferencia, la llamada se traba y otros teléfonos que compartan el número de directorio de línea octal no puede tomar la llamada.
- Las llamadas perdidas (llamadas no contestadas) no se muestran por defecto.
- Se necesita un anexo compartido de línea octal para activar la función Conference Barge (cBarge). Para obtener más información, consulte **Conference Barge, página 422**.

Se aplican las siguientes limitaciones a las líneas octales:

- Las líneas octales no admiten sobrecapas. Esto significa que los anexos que se configuran para funciones como Conferencias o Conference Barge (cBarge) no puede tener sobrecapas.
- Las líneas octales sólo están disponibles si la versión del IOS de Cisco en el UC500 es 12.4(20)T ó posterior y la versión de Unified Communications Manager Express (CUCME) es 7.0 ó posterior. Se recomienda la actualización al más reciente del Paquete de software para UC500.
- No todos los modelos de teléfonos IP de Cisco admiten líneas octales.
- Los modelos de teléfonos IP Modelos 7920, 7902, 7931G, CP-52xG, CP-52xSG y de la serie SPA500 de Cisco no admiten líneas octales.
- Los puertos ATA y FXS analógicos de Cisco no admiten líneas octales.

Correo de voz y notificaciones

Los temas de esta sección entregan instrucciones para configurar el correo de voz y las notificaciónes:

Para configurar las opciones de Correo de voz y buzones, seleccione **Configurar** > **Telefonía** > **Usuarios y anexos**> **Correo de voz** en la barra de funciones. Consulte los siguientes temas para obtener información sobre cómo activar y configurar las funciones de correo de voz.

- **Visión general**
- **Pautas generales**
- **Instalación**
- **Buzones**
- **Notificaciónes**

Visión general

En la ventana Correo de voz, se realiza la configuración de correo de voz básico para el tisio, se ve y edita la cantidad de almacenamiento de correo de voz para cada buzón.

Pautas generales

Las siguientas pautas se aplican a los buzones de correo de voz y notificaciones:

- Al agregar usuarios y teléfonos por medio del Asistente de configuración de telefonía, se crean buzones de voz si está marcada la opción de activar el correo de voz para el usuario.
- Los usuarios pueden acceder a su correo de voz desde cualquier teléfono del sistema simplemente marcando el anexo del correo de voz o el número de acceso PSTN al correo de voz. Se les solicita que indiquen su PIN de correo de voz para acceder el buzón de correo. El PIN por defecto para el acceso al correo de voz es 1234. Los usuarios que accedan a su correo de voz por primera vez deberán cambir su PIN.
- Al agregar usuarios por medio de UI en modo experto o carga de archivos .XML, los buzones personales se crean inicialmente en el sistema para usuarios cuando la configuración de **Desvío ocupado** o **Desvío sin respuesta** para cualquier anexo Normal está determinada para ir al correo de voz. Esta

configuración se realiza en la ficha Anexos de usuarios de la ventana Editar teléfono (**Configurar** > **Telefonía** > **Usuarios y anexos**> **Usuarios y teléfonos**> **Editar teléfono**).

- La configuración por defecto tanto para **Desvío ocupado** y **Desvío sin respuesta** es Correo de voz. Ello significa que si se agregar un usuario y no se modifica ninguna de estas configuraciones cuando se agrega el usuario, se crea un buzón de voz automáticamente para dicho usuario. Se puede desactivar el buzón de correo de voz más tarde en la ficha Anexos de usuarios de la ventana Editar teléfono (**Configurar** > **Telefonía** > **Usuarios y anexos**> **Usuarios y teléfonos**> **Editar teléfono**).
- Cuando se cambia la configuración de **Desvío ocupado** y **Desvío sin respuesta** de los usuarios exitentes desde Correo de voz a una opción diferente, el buzón del usuario permanece en el sistema. Si ya no desea que el usuario tenga un buzón de correo de voz, debe desactivarlo manualmente en la ficha Anexos de usuarios de la ventana Editar teléfono (**Configurar** > **Telefonía** > **Usuarios y anexos**> **Usuarios y teléfonos**> **Editar teléfono**).
- Puede crearse un buzón personal por usuario y puede asociarse con cualquiera de los anexos Normales configurados para el usuario o un anexo (compartido) personal.
- Se crean Buzones de entrega generales (GDM) para los anexos compartidos, grupos de llamado y grupos de envío de llamadas cuando se configura **Desvío sin respuesta** como Correo de voz pare el grupo o anexo compartido. También se puede seleccionar crear un buzón (compartido) personal para un anexo compartido.

SUGERENCIA: La vista Tablero (**Inicio** > **Tablero**) entrega un elemento de **Estado deCorreo de voz** que muestra un resumen de la utilización del almacenamiento de correo de voz por buzón, información por cada una de ellos y su estado.

Instalación

En la ficha Configuración, se configuran estos parámetros de correo de voz básicos para un sitio:

- Anexo de acceso al correo de voz y número PSTN
- Prefijo para la transferencia directa al correo de voz
- Configuración global del sitio para activar la notificación de mensajes de correo de voz entrantes por correo electrónico y/o teléfono
- Activar las funciones VoiceView Express y LiveReply para el sitio

Para configurar el correo de voz del sistema, complete los campos en la ficha Configurar como se describe a continuación y haga clic en **Aceptar**.

Configuración	Descripción
Número de acceso	
Anexo de acceso a correo de voz	Número de anexo interno para el acceso al correo de voz. El Anexo de acceso al correo de voz por defecto es 399.
Número PSTN del acceso al correo de voz	*Opcional*. Número PSTN externo para el acceso al correo de voz. Debe ser un número E.164 íntegro. Es el número que quien llame desde el exterior marcará para llegar al correo de voz. El Número PSTN externo para el acceso al correo de voz puede comenzar con un carácter "+".
Funciones de correo de voz	
VoiceView Express	**VoiceView Express** permite que los usuarios telefónicos interactúen con su buzón de voz Unity Express de Cisco utilizando su pantalla de teléfono IP de Cisco y las teclas en el teléfono. Los usuarios pueden administrar las opciones de buzón personal, administrar notificaciones, enviar, escuchar, grabar y administrar mensajes de correo de voz. La función entrega una alternativa a la TUI (Interfaz de usuario telefónico) una interfaz de Internet para estas tareas. Por defecto, esta función está activada.

Configuración	Descripción
Live Reply	**Live Reply** permite que los usuarios de correo de voz de Unity Express de Cisco que escuchen sus mensajes de correo de voz por teléfono o por Voice View Express puedan responder el mensaje de otro usuario al presionar 4-4. Cuando se invoca Live Reply, Unity Express de Cisco intenta establecer una llamada entre ambas partes. Si el intento tiene éxito, el usuario de correo de voz se conecta a la parte llamada o la llamada de voz se desvía según las reglas definidias por la parte llamada. Después que termine la llamada, se desconecta la conexión inicial al correo de voz. El usuario de correo de voz no se devuelve a su sesión de correo de voz. Para revisar otros mensajes del correo de voz después de una sesión Live Reply exitosa, el usuario debe volver a marcar el número de acceso del correo de voz. Por defecto, esta función está activada.

Configuración	Descripción
Reproduzca la ID de quien llama para los Mensajes entrantes	Activa o desactiva la reproducción de la ID de quien llama para los mensajes entrantes del correo de voz. Cuando se activa **Reproducir la ID de quien llama para los mensajes entrantes** iy se recibe un mensaje de correo de voz, dependiendo si la llamada entrante es de un número interno o externo: ▪ **Llamadas internas**. Si la información de ID de quien llama coincide con el directorio local, el sistema reproduce el nombre de quien llama a partir del directorio local cuando el receptor escucha el mensaje. ▪ **Llamadas externas**. Si la información de ID de quien llama no coincide con el directorio local, el sistema reproduce el número de teléfono de quien llama cuando el receptor escucha el mensaje. Para las llamadas externas, el sistema no verifica que la información de ID de quien llama sea válida. Esa función depende de la oficina central (CO) y de la configuración del enlace entrante. Una llamada externa es aquella que viene de cualquier número de teléfono que no esté indicado en el directorio local del usuario. Los posibles orígenes de las llamadas externas con la empresa de teléfonos local, un teléfono IP o un gateway H.323. Estas fuentes deben configurarse para presentar la información de ID de quien llamas al sistema de correo de voz.

Configuración	Descripción
Transferencia directa	

Configuración	Descripción
Activar transferencia directa al correo de voz	Marque esta opción para activar **Transferencia directa a correo de voz** y especifique un **Prefijo de transferencia de correo de voz**. El **Prefijo de transferencia a correo de voz** puede ser un número de 1 a 9. El valor por defecto es 6. El prefijo lo utiliza la Contestadora automática y los usuarios telefónicos que no tienen teclas para transferir las llamadas al correo de voz en su teléfono. El prefijo no puede ser el mismo que el código de acceso PSTN para las llamadas externas o el primer dígito de un anexo interno. Cuando se activa esta función, la Contestadora automática se actualiza para incluir una opción para la transferencia directa al correo de voz. Cuando se activa o desactiva la **Transferencia directa a correo de voz**, se reinician los teléfonos IP y se agregan o quitan teclas. Cuando se activa **Transferencia directa a correo de voz** , los usuarios de teléfonos IP con la tecla **TrnsferVM** en sus teléfonos puede transferir una llamada directamente a un usuario o buzón de voz de grupo siguiendo estos pasos: 1. Presionar la tecla **TrnsferVM** en el teléfono. 2. Especificar el anexo de correo de voz de usuario o grupo. 3. Presionar la tecla **TrnsferVM** de nuevo para realizar la transferencia. Los usuarios telefónicos sin una tecla de transferencia de correo de voz transfieren una llamada al correo de voz siguiendo estos pasos: 1. Presionar la tecla **Trnsfer**. 2. Especifique el prefijo de transferencia de correo de voz, seguido del anexo del usuario. por ejemplo, si el prefijo de transferencia de correo de voz es 6 y se desea transferir a correo de voz para el anexo 201, se debe presionar **Trnsfer**, seguido de 6201.

Configuración	Descripción
Notificación de correo de voz Active y configure los parámetros del sitio global para las notificaciones de correo de voz.	
Activar notificación por correo de voz	Por defecto, la notificación de mensajes de correo de voz está desactivada. Se debe verificar la opción Activar notificación de correo de voz antes de poder configurar el sitio para las notificaciones por correo de voz y teléfono, o active las notificaciones para sus usuarios. Desactivar notificaciones de correo de voz Si las notificaciones de correo de voz están activadas y se desmarca esta opción, el CCA restablecerá la configuración de notificación.

Configuración	Descripción
Calendario de notificación	Seleccione cuándo el sistema enviará la notificación: ▪ Haga clic en **8 AM a 5 PM** Lunes a Viernes o ▪ Haga clic en **24 Horas** al día, 7 días a la semana.
Notificación por correo electrónico	Realice esta configuración para activar y configurar las notificaciones de correo de voz por correo electrónico. ▪ Marque la opción **Activar notificación por correo electrónico** para activar las notificaciones de correo de voz por correo electrónico para el sitio. ▪ En el campo **Dirección de respuesta del correo electrónico saliente:** escriba la dirección de correo electrónico que aparecerá en el Formulario: campo para notificaciones de correo electrónico enviadas desde el sistema de correo de voz. ▪ En el campo **Dirección del servidor SMTP**, escriba el nombre del host o dirección IP del servidor SMTP que el sistema de correo de voz usará para enviar las próximas notificaciones. Para usar un nombre de host para esta configuración, el *DNS debe estar activado*. ▪ Escriba el número del **Puerto del servidor SMTP**. ▪ Si el servidor SMTP pide autenticación, marque la opción **Requerir autenticación** y escriba el nombre y contraseña del usuario para el servidor SMTP.
Notificación por teléfono	Debe marcarse la opción **Permitir que los receptores de notificaciones accedan al inicio de sesión en el buzón de correo** si se desea activar el envío de notificaciones de mensajes de correo de voz a los teléfonos. Por defecto, esta opción está desactivada.

Buzones

En la ficha buzones de correo se puede ver la información de almacenamiento y el resumen para los buzones personales y grupales.

Configure el buzón como se describe a continuación, y haga clic en **Aceptar** después de realizar los cambios.

Campo	Descripción	
Almacenamiento	Almacenamiento de correo de voz disponible y utilizado, en minutos, para el sistema.	
Resumen	Información de resumen para cada buzón de voz.	
	Nombre (ID de usuario)	ID del usuario telefónico, ID de grupo (por ejemplo, hunt1 o blast1) o Línea compartida, para el buzón seleccionado.
	Anexo	Anexo del usuario, anexo piloto del grupo de búsqueda o de envío de llamadas, o anexo de línea compartida para el buzón seleccionado.
	Buzón	Estado del buzón, ya sea Activo o Ninguno.
	Tamaño	Tamaño del buzón, en minutos.

Campo	Descripción	
Parámetros de buzón de	Ver o editar la configuración de buzón para el buzón de voz seleccionado.	
	Anexo	Si es un buzón personal, este campo muestra el anexo del usuario asociado con este buzón.
	Tipo	Personal o GDM (Buzón de entrega general). Se puede cambiar un buzón de correo GDM que se crea para un anexo compartido a un buzón de correo (compartido) personal cambiando el tipo de éste a personal, y seleccionando un usuario de la lista desplegable. Sólo usuarios con este anexo compartido que no tengan actualmente un buzón de voz Personal aparecen en la lista. Un buzón de correo (compartido) personal no puede cambiarse a un buzón GDM. Si el Tipo de buzón para un anexo compartide es (Compartido) personal, la única forma de cambiarlo de vuelta a GDM es eliminar el usuario asociado al buzón (compartido) personal, aplicar la configuración y luego volver a crear al usuario.
	Tamaño	Ver o editar la cantidad de almacenamiento asignado a este buzón, desde 4 a 90 minutos. Por defecto, son 12 minutos.

Notificaciónes

Si las notificaciones de correo de voz se activan y configuran para este sitio, las opciones de la ficha Notificaciones permiten seleccionar el anexo que tenga un buzón de correo de voz y realizar la configuración para las notificaciones por correo electrónico y teléfono.

El correo de voz y notificaciones de mensajes de fax se puede enviar a un teléfono (por ejemplo, el teléfono del usuario de casa, teléfono celular, o de otro tipo de trabajo número) o de su buzón de correo electrónico.

Para cada usuario, se puede:

- Seleccionar si se activan las notificaciones por teléfono, correo electrónico o ambas.
- Seleccione si los mensajes de voz y facsímiles se adjuntan a los correos electrónicos de notificación (los facsímiles se adjuntan como archivos con formato .TIFF).
- Especifique un nivel de notificación separado para las notificaciones por correo electrónico y teléfono. Puede seleccionar si se envían las notificaciones para todos los mensajes de correo de voz o sólo para los marcados como "Urgente" por el remitente. La opción Urgente se aplica sólo a correos de voz, no a facsímiles.

CCA no admite las siguientes funciones de notificación de correo de voz:

- Calendario de notificación
- Texto del prefijo y sufijo del mensaje de notificación
- Límite de tiempo de conexión
- La table de restricción para la especificación de números de teléfono que los usuarios de correo de voz pueden usar para enviar notificaciones de mensajes
- Notificación de mensajes en cascada

Para agregar usuarios de notificación de correo de voz o editar la configuración de notificación para los usuarios existentes, siga estos pasos.

PASO 1 Seleccione **Configurar** > **Telefonía** > **Usuarios y anexos** > **Correo de voz** y seleccione la ficha Notificaciones.

PASO 2 Si se está agregando un nuevo usuario y anexo, haga clic en **Agregar**.

PASO 3 Para editar la configuración para un usuario y anexo existente, seleccione un usuario de la lista y haga clic en **Editar**.

PASO 4 Realice la configuración como se describe en **Agregar o editar al usuario de notificaciones, página 389**.

PASO 5 Haga clic en **Aceptar**.

Agregar o editar al usuario de notificaciones

Aparece el diálogo Agregar/editar usuario de notificaciones cuando se hace clic en **Agregar** o en **Editar** en la ficha Notificación de la ventana Correo de voz (**Configurar** > **Telefonía** > **Usuarios y anexos** > **Correo de voz**).

Para configurar la notificación de correo de voz por correo electrónico y teléfono para un anexo, realice la configuración descrita a continuación y haga clic en **Aceptar**.

Configuración	Descripción
Anexo	Seleccione un anexo disponible de la lista desplegable. Sólo se indican anexos que tengan un buzón de correo de voz. Puede tratarse de buzones de correo de voz personales o grupales (GDM).
Nombre de usuario (sólo lectura)	Cuando usted elige una extensión, nombre y apellido del usuario y su ID de usuario aparece aquí. Si es un anexo compartido, se muestra la línea compartida aquí.
Notificación por correo electrónico Configure las notificaciones de correo de voz y facsímil para el buzón de voz asociado con este anexo.	
Notificar al usuario de nuevo correo de voz por correo electrónico	Cuando se marca esta opción, la notificación de nuevos mensajes de correo de voz o facsímiles se activa para este usuario.
Dirección de correo electrónico	Escriba la dirección de correo electrónico a la que se envían las notificaciones. La dirección de correo electrónico puede tener hasta 129 caracteres.

Configuración	Descripción
Adjunto	Cuando se marca la opción **Adjuntar archivo de correo de voz a mensaje de correo electrónico**, el mensaje de correo de voz o facsímil se adjunta al correo electrónico de notificación. Cada mensaje de correo de voz se adjunta como archivo .WAV. El formato del archivo .WAV es G711 mu-law, 8 KHz, 8-bit mono. Los facsímiles se adjuntan en formato de archivos .TIFF. Por defecto, esta opción está desactivada. Loa mensajes privados nunca se adjuntan a la notificación por correo electrónico.
Nivel de notificación	Seleccione una de los siguientes niveles de notificación: ▪ Correo de voz urgente solamente (no se aplica a facsímiles). ▪ Todo el correo de voz. Seleccione esta opción si está configurada la función T.37 Facsímil a correo para su sistema y se desea que los usuarios reciban notificación de facsímiles entrantes por correo electrónico con el facsímil adjunto al mensaje de correo electrónico.
Notificación por teléfono	
Notificar al usuario de nuevo correo de voz por teléfono	Cuando se marca esta opción, la notificación de nuevos mensajes de correo de voz o facsímiles se activa para este usuario.
Tipo de teléfono	Seleccione uno de los siguientes tipos de teléfonos: ▪ Teléfono celular ▪ Teléfono de la casa ▪ Teléfono del trabajo

Configuración	Descripción
Número de teléfono	Escriba número de teléfono al que se enviarán las notificaciones. Al especificar un número externo, asegúrese de incluir todo código de acceso, si es necesario.
Dígitos adicionales	El sistema marca estos dígitos cuando se contesta la llamada saliente. Estos dígitos se tratan como dígitos DTMF. Por ejemplo, dígitos adicionales pueden usarse al enviar llamadas a un localizador o sistema de respuestas automáticas. Es posible especificar hasta 64 dígitos. Los dígitos adicionales pueden consistir en dígitos entre 0 y 9, # (signo de número), asterisco (*) y signo más (+).
Nivel de notificación	Seleccione una de los siguientes niveles de notificación: ▪ Correo de voz urgente solamente (no se aplica a facsímiles). ▪ Todo el correo de voz. Seleccione esta opción si está configurada la función T.37 Facsímil a correo para su sistema y se desea que los usuarios reciban notificación de facsímiles entrantes por correo electrónico con el facsímil adjunto al mensaje de correo electrónico.

Ubicación con número individual (SNR)

Esta ventana aparece cuando se selecciona **Configurar** > **Telefonía**> **Usuarios y anexos**> **Ubicación con número individual** en la barra de funciones.

Ubicación con número individual (SNR) entrega a los usuarios la posibilidad de ser localizados en dos números: un anexo regular en su teléfono IP y en un número PSTN. Se admiten interfaces BRI, PRI, FXO y SIP.

NOTEA Para los números SNR que van sobre los troncales SIP, la ID de quien llama puede no reflejar la ID original de quien llama, porque esta ID se determina por parte del ITSP. Por lo general, la ID de quien llama será la estación o el número PSTN principal configurado para el troncal SIP. La mayoría de los ITSP exigen que las ID de quien llama se mapeen explícitamente a sus cuentas para evitar el fraude. Si la ID de quien llama no se sobreescribe con la ID de quien llama original que requiere el ITSP, la llamada al número SNR fallará.

- **Visión general**
- **Limitaciones**
- **Requerimientos de la plataforma SBCS**
- **Procedimientos y parámetros de configuración**

Visión general

La función Ubicación con número individual (SNR) permite que los usuarios telefónicos contesten las llamadas entrantes en su teléfono IP de escritorio o en una ubicación remot, como un teléfono celular, o tomar llamadas en curso en el teléfono de escritorio o en el teléfono remoto sin perder la conexión. Esto le permite a quien llaman utilizar un solo número para ubicar al usuario telefónico. Las llamadas que no se contestan se reenvían al correo de voz.

Los destinos remotos pueden incluir los siguientes dispositivos:

- Teléfonos móviles (celulares)
- Smart phones
- Teléfonos IP que no pertenezcan al mismo router CME unificado de Cisco que el teléfono de escritorio
- Números de teléfono personales de PSTN
- Las interfaces PSTN admitidas incluyen PRI, BRI, SIP y FXO.

Para las llamadas entrantes al anexo SNR, CME unificado de Cisco hace sonar el teléfono IP de escritorio primero. Si el teléfono IP no contesta dentro del lapso configurado, hace sonar el número remoto configurado mientras sigue llamando al teléfono IP. Las llamadas no contestadas se envían al número de correo de voz configurado.

El usuario del teléfono IP tiene las siguientes opciones para administrar las llamadas al anexo SNR:

- **Retirar la llamada del teléfono remoto**. Retire manualmente la llamada hasta el anexo SNR presionando la tecla **Reanudar**, la que desconecta la llamada del teléfono remoto.
- **Enviar la llamada al teléfono remoto.** Envíe la llamada al teléfono remoto utilizando la tecla **Movilidad**. Mientras se conecta a la llamada, el usuario telefónico puede presionar la tecla **Movilidad** y seleccionar "Enviar llamada a celular". La llamada de reenvía al teléfono remoto.
- **Activar o desactivar Ubicación con número individual**. Mientras el teléfono IP esté inactivo, el usuario puede activar o desactivar la función SNR utilizando la tecla Movilidad. Si el usuario desactiva SNR, el sistema no llama al número remoto.

Los usuarios de teléfonos IP pueden modificar su propia configuración SNR desde el teléfono utilizando el menú disponible con el botón de función **servicios**. Se debe activar la función en el teléfono para permitir que un usuario telefónico acceda a la interfaz del usuario.

Limitaciones

Se aplican las siguientes limitaciones a la configuración y funciones de SNR:

- Cada teléfono IP sólo admite un número de SNR.
- No se admite el uso simultáneo de la aplicación T.37 Detección de facsímil y SNR.
- No se puede configurar SNR en un anexo que sea miembro de un grupo de búsqueda.
- No se admite la función SNR para lo siguiente:
  - Teléfonos FXS análogos controlados por SCCP
  - Llamadas con video
  - Teléfonos SCCP que no tienen teclas En algunos casos, SNR puede configurarse en estos teléfonos, pero ya que no tienen tecleas, no puede usarse la función Movilidad.

Parfa obtener mayor información acerca de las funciones y limitaciones de SNR, consulte la *Guía del Administrador de sistemas de Communications Manager Express de Cisco*, disponible en Cisco.com en la siguiente URL:

www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cmeadm.html

Requerimientos de la plataforma SBCS

Se admite esta función en CME 7.1, disponible con el paquete de software 7.1.1-EA ó posterior para UC500.

Procedimientos y parámetros de configuración

Para activar SNR para uno o más usuarios de teléfonos o editar la configuración para los usuarios de SNR, siga estos pasos.

PASO 1 Seleccione **Configurar> Telefonía > Usuarios y anexos > Ubicación con número individual** en la barra de funciones.

PASO 2 Haga clic en **Agregar** o **Editar**. Aparece la ventana Agregar o Modificar usuario de SNR.

PASO 3 Configure los usuarios de SNR como se describe en la sección **Agregar un usuario SNR, página 394** o en la sección **Modificación de un usuario SNR, página 395**.

PASO 4 Haga clic en **Aceptar**.

Agregar un usuario SNR

Esta ventana aparece cuando hace clic en **Agregar** en la ventana Ubicación con número individual.

Para agregar un usuario de SNR, siga estos pasos:

PASO 1 Realice esta configuración para cada usuario de SNR.

Configuración	Descripción
Nombre de usuario	Seleccione un usuario de la lista desplegable.
Dirección MAC	*Sólo lectura*. Este campo muestra la dirección MAC del teléfono asociado con el anexo del usuario que se selecciona al crear el usuario de SNR.

Configuración	Descripción
Anexo	Cuando se selecciona un usuario, el menú muestra las extensiones disponibles en el teléfono del usuario que se puede utilizar para SNR. Si el anexo que se selecciona es una línea compartida, el texto (línea compartida) aparece a la derecha del anexo. Seleccione la extensión en el teléfono del usuario a utilizar para SNR. Si el usuario seleccionado ya tiene SNR configurado en un anexo en su teléfno, se muestra un mensaje de advertencia. Sólo puede configurarse un anexo por teléfno para el SNR.
Destino remoto	Escriba o edite el número de teléfono para el destino remoto. Cuando se especifica el número del teléfono de destino remoto, indique el número exactamente como se discaría, incluyendo cualquier código de acceso, códigos para llamadas de larga distancia y cualquier otro dígito para discar que sea necesario.
Configuración de retraso y límite de tiempo	
Retraso antes de discar al destino remoto (segundos)	El retraso especifica el número de segundos que la llamada suena en el teléfono IP antes de sonar en el teléfono remoto. Especifique un número entre 1 y 10 segundos. El valor por defecto es 5 segundos.
Retraso del reenvío de llamadas al correo de voz (seg.)	Número de segundos para dejar que la llamada suene en el teléfono IP y en el teléfono remoto antes de transferir la llamada al correo de voz. Especifique un número entre 5 y 60 segundos. El valor por defecto es 30 segundos.

PASO 2 Haga clic en **Aceptar**.

Modificación de un usuario SNR

Aparece este diálogo cuando se hace clic en **Editar** en la ventana SNR (**Configurar** > **Telefonía** > **Usuarios y anexos** > **Ubicación con número individual**).

Sólo se puede editar el número de destino remoto y la configuración del límite de tiempo de SNR.

Si desea cambiar el anexo asociado con un usuario SNR, se debe eliminar al usuario SNR, volver a agregarlo y seleccionar un anexo diferente.

Para modificar la configuración de usuarios SNR, siga estos pasos:

PASO 1 Determine la configuración del usuario SNR según se describe en la siguiente tabla.

Configuración	Descripción
Nombre de usuario	*Sólo lectura*. Este campo muestra el nombre y apellido del usuario asociado con este anexo.
Dirección MAC	*Sólo lectura.* Este campo muestra la dirección MAC del teléfono asociado con este anexo del usuario SNR.
Anexo	*Sólo lectura*. Este campo muestra el anexo que se seleccionó al agregar este usuario SNR.
Destino remoto	Edite el número de teléfono para el destino remoto. Cuando se edite el número del teléfono de destino remoto, indique el número exactamente como se discaría, incluyendo cualquier código de acceso, códigos para llamadas de larga distancia y cualquier otro dígito para discar que sea necesario.
Miembros con línea compartida	Sólo lectura. Si el anexo es una línea compartida, se muestra la lista de usuarios.
Configuración de retraso y límite de tiempo	
Retraso antes de discar al destino remoto (segundos)	El retraso especifica el número de segundos que la llamada suena en el teléfono IP antes de sonar en el teléfono remoto. Especifique un número entre 1 y 10 segundos. El valor por defecto es 5 segundos.

Configuración	Descripción
Retraso del reenvío de llamadas al correo de voz (seg.)	Número de segundos para dejar que la llamada suene en el teléfono IP y en el teléfono remoto antes de transferir la llamada al correo de voz. Especifique un número entre 5 y 60 segundos. El valor por defecto es 30 segundos.

PASO 2 Haga clic en **Aceptar**.

Discados rápidos del sistema

Para configurar los Discados rápido del sistema, seleccione **Configurar** > **Telefonía** > **Usuarios y anexos** > **Discado rápido del sistema** en la barra de funciones.

En la ventana Discado de velocidad del sistema, se puede definir números de discado rápido local.

Visión general

Puede crearse una lista de los números llamados frecuentemente para todos los teléfonos. Un usuario telefónico puede marcar rápidamente un número de discado rápido.

Los usuarios de teléfonos acceden a estos discados rápidos desde el menú **Servicios locales** > **Discado rápido local** en su teléfono.

Se puede agregar, editar o eliminar las entradas de discado de velocidad. Las entradas de lalista pueden desplazarse hacia arriba y hacia abajo por la lista y aparecen en la pantalla del teléfono en el orden en que se indican. Puede definirse un máximo de 32 números llamados frecuentemente en la lista.

Procedimientos

Para activar un menú de discado rápido local para todos los teléfonos IP, realice los siguientes pasos:

PASO 1 Haga clic en **Agregar**.

PASO 2 En el campo **Nombre**, especifique el nombre rápido.

PASO 3 En el campo **Número de teléfono**, especifique el número para el discado rápido.

PASO 4 Para reordenar un número de discado rápido local en la lista, seleccione la entrada y haga clic en la flecha hacia arriba o hacia abajo. Los números se indican en el orden en que se muestran en el teléfono.

PASO 5 Para quitar un número del discado de velocidad local del menúi, seleccione la entrada en el menú y haga clic en **Eliminar** en la casilla Discados rápidos locales.

Si la lista ha llegado al máximo número de entradas permitidos, se desactiva el botón **Agregar**.

12

Grupos telefónicos

Esta sección entrega instrucciones para configurar los siguientes tipos de grupos telefónicos:

- **Grupos de llamado**
- **Llamar a grupos de envío**
- **Grupos de contestación**
- **Grupos de localización**

Para configurar grupos telefónicos, seleccione **Configurar** > **Telefonía** > **Grupos telefónicos** en la barra de funciones.

Grupos de llamado

Para configurar grupos de llamado, seleccione **Configurar** > **Telefonía** > **Grupos de telefónicos** > **Grupos de llamado** en la barra de funciones.

Visión general

Utilice los grupos de llamado para administrar la distribución de llamadas enrantes a un grupo definido previamiente de anexos (miembros). El tipo de grupo de llamado determina el orden en que los miembros del grupo reciben las llamadas.

Hasta 10 grupos de llamado pueden configurarse en el sistema. Caga grupo de llamado debe tener, al menos, un miembro y hasta 32 de ellos.

Una vez que se configuren los grupos de llamado, quedan disponibles para seleccionarlos como destinos para el enrutamiento de llamadas entrantes, la Contestadora automática, destinos de envío de llamadas y otras funciones de telefonía.

Cuando se configura un grupo de llamado, se agrega la tecla **HLog** a los teléfonos miembros. Los miembros de grupos de llamado pueden iniciar o cerrar sesión en el grupo usando la tecla **HLog**. La tecla **HLog** aparece en el teléfono del grupo de llamado cuando una llamada entrante al grupo de búsqueda se recibe en el teléfono. Los usuarios también pueden acceder a esta tecla desde la pantalla principal del teléfono presionando la tecla **más**. La tecla **HLog** reemplaza el uso de DnD (No molestar) . DnD es menos flexible, ya que deja al suscritpor no disponible para todas las llamadas, no sólo las llamadas al grupo de llamado.

Limitaciones

La siguiente limitación se aplica a la configuración de grupos de llamado:

- Un teléfono que tiene SNR activado no puede ser un miembro de un grupo de llamado.

Procedimientos

Para activar y configurar un grupo de llamado, realice la configuración como se describe a continuación, y haga clic en **Aceptar** o **Aplicar**.

Configuración	Descripción
Activar	Cuando se marca esta casilla, se activa el grupo de llamado asociado.
Nro. ext	Número piloto para este grupo de llamado. Es el anexo que se marca para llegar al grupo de llamado. Utilice el anexo por defecto para el número piloto haga clic en el campo y edítelo.
Descripción	*Opcional*. Descripción del texto que identifica este grupo de llamado. Esta descripción sólo se usa en la ventana Grupo de llamado. En otras partes de la interfaz del usuario de CCA, al grupo de llamado lo identifica su número y anexo piloto, por ejemplo, hunt1 (502).

Configuración	Descripción
Tipo de búsqueda	Determina el orden en que los miembros del grupo de llamado reciben las llamadas. Seleccione una de las siguientes opciones: ▪ **Secuencial**; la búsqueda de llamados siempre comienza con el número piloto del grupo y sigue con cada número del grupo en el orden que se indican, de arriba hacia abajo, en la lista Miembros. ▪ **Mayor desocupación**; las llamadas van al número del directorio que ha estado desocupado por más tiempo, de acuerdo con la marca horaria de la llamada más reciente al grupo de llamado que dicho anexo haya tomado. Si dicho anexo no está disponible, la búsqueda continúa con el siguiente anexo del grupo. ▪ **Azar**; grupo de llamado en el que el primer número llamado se selecciona al azar en la lista.
Miembros	Define los miembros del Grupo de llamado. Son todos los números que pueden sonar cuando entra una llamada al número piloto. 1. Haga clic en **Miembros** para mostrar la lista de usuarios Disponibles y Seleccionado en la parte inferior de la ventana Grupos de llamado. 2. Utilice los botones de flechas **Agregar** y **Quitar** para transferir elementos entre la lista de miembros Disponible y Seleccionados. Utilice CTRL-clic y SHIFT-clic para seleccionar múltiples miembros y desplazarlos entre las listas. 3. Utilice las flechas **Hacia arriba** y **Hacia abajo** para especificar el orden en que las llamadas se rutean hacia el Grupo de llamado.
Límite de tiempo (seg.)	Número de segundos después de los que se redirecciona una llamada no contestada al siguiente número de una lista de grupo de llamado de voz, desde 5 a 20 segundos.

Configuración	Descripción
Desvío sin respuesta	Destino para enviar las llamadas no contestadas para el grupo de llamado. Se puede seleccionar **Ninguno**, **Contestadora automática**, **Correo de voz**, **Anexo**, **Grupo de llamado**, **Grupo de envío**, **B-ACD**, u **Otro número**. Si se selecciona **Correo de voz**como el destino de **Desvío sin respuesta**, se crea un Buzón de entrega general (GDM) para el grupo. Para ver la información del buzón GDM o cambiar el tamaño del buzón, vaya a la ventana **Configurar** > **Telefonía** > **Correo de voz** y seleccione la ficha **Buzones**.

Llamar a grupos de envío

Para configurar Grupos de envío de llamadas, seleccione **Configurar** > **Telefonía** > **Grupos de telefónicos** > **Llamar a grupos de envío** en la barra de funciones.

Visión general

Un grupo de envío de llamadas es un tipo especial de grupo telefónico en el que las llamadas a un número piloto especificado campanillean simultáneamente en múltiples teléfonos. Esta función también puede utilizarse para configurar un escenario de Ubicación con número individual en el que una llamada al anexo del teléfono del usuario campanillee en otro número (por ejemplo, un número de teléfono celular o uno privado) o en un anexo diferente.

Hasta 10 grupos de envío de llamadas pueden configurarse en el sistema. Cada grupo de envío de llamadas debe tener, al menos, dos miembros y puede contener hasta 32 miembros.

Una vez que se configuren los grupos de envío de llamadas, quedan disponibles para seleccionarlos como destinos para el enrutamiento de llamadas entrantes, la Contestadora automática, destinos de envío de llamadas y otras funciones de telefonía.

Cuando se configura un grupo de envío, se agrega la tecla **HLog** a los teléfonos miembros. Los miembros de grupos de llamado pueden iniciar o cerrar sesión en el grupo de envío de llamadas usando la tecla **HLog**. La tecla **HLog** aparece en todos los teléfonos del grupo de envío cuando se recibe una llamada entrante al

grupo de envío. Los usuarios también pueden acceder a esta tecla desde la pantalla principal del teléfono presionando la tecla **más**. La tecla **HLog** reemplaza el uso de DnD (No molestar) . DnD es menos flexible, ya que deja al suscritpor no disponible para todas las llamadas, no sólo las llamadas al grupo de envío.

Procedimientos

Para activar y configurar un grupo de envío de llamadas, realice la configuración como se describe a continuación, y haga clic en **Aceptar** o **Aplicar**.

Configuración	Descripción
Activar	Cuando se marca esta casilla, se activa el grupo de envío asociado.
Nro. ext.	Número piloto para este grupo de envío de llamadas. Es el anexo que se marca para llegar al grupo de llamado de envío de llamadas. Utilice el anexo por defecto para el número piloto o haga clic en el campo y edítelo.

Configuración	Descripción
Miembros	Define los miembros del Grupo de envío de llamada. Son todos los números que pueden sonar cuando entra una llamada al número piloto. 1. Haga clic en **Miembros** para mostrar la lista de usuarios Disponibles y Seleccionado en la parte inferior de la ventana Grupos de envío de llamadas. 2. Utilice los botones de flechas **Agregar** y **Quitar** para transferir miembros entre la lista de miembros Disponible y Seleccionados. Utilice CTRL-clic y SHIFT-clic para seleccionar múltiples miembros y desplazarlos entre las listas. Para agregar un número PSTN externo (por ejemplo, un número celular o privado) a la lista de miembros Disponibles y desplazarlo a la lista Seleccionados: 1. En el campo **Otro número**, especifique el número telefónico exactamente como usted lo marcaría, incluyendo cualquier código de acceso (hasta 16 dígitos). 2. Haga clic en el botón **Agregar** a la derecha del campo **Otro número** para desplazarlo a la lista Disponible. 3. Haga clic en el botón de flecha **Agregar** para trasladar el Otro número que acaba de agregarse a la lista Seleccionado. Par quitar un número externo de la lista Seleccionados, haga clic en el botón de flecha **Quitar** para devolverlo a la lista Disponible. Una vez que se cierra la ventana Grupos de envío de llamadas o se selecciona un Grupo de envío de llamadas diferente para configurarlo, cualquier número externo agregado a la lista Disponible, pero no desplazado a la lista Seleccionado se elimina de la lista Disponible. Cuanso se abre posteriormente la lista de selección Miembro, estos números telefónicos externos no aparecen en la lista Disponible.

Configuración	Descripción
Límite de tiempo (seg.)	Número de segundos después de los que se redirecciona una llamada no contestada al destino especicado en **Desvío sin respuesta**, entre 5 y 20 segundos. El Límite de tiempo por defecto es 16 segundos. **IMPORTANTE** El valor **Límite de tiempo** para el grupo de envío de llamadas debe ser iferior al valor del límite de tiempo de CFNA para cualquiera de sus anexos. Puede ser necesario reducir el valor del Límite de tiempo para un Grupo de envío de llamadas o elever el valor del límite de tiempo de CFNA para los anexos miembros y asegurarse que se cumpla con este requisito.
Desvío sin respuesta	Destino para enviar las llamadas no contestadas para el grupo de llamado. Se puede seleccionar **Ninguno**, **Contestadora automática**, **Correo de voz, Anexo**, **Grupo de llamado**, **Grupo de envío**, **B-ACD**, u **Otro número**. Si se selecciona **Correo de voz**como el destino de **Desvío sin respuesta**, se crea un Buzón de entrega general (GDM) para el grupo. Para ver la información del buzón GDM o cambiar el tamaño del buzón, vaya a la ventana **Configurar** > **Telefonía** > **Correo de voz** y seleccione la ficha **Buzones**.
Número	Número para el tipo de destino seleccionado para **Desvío sin respuesta**: ▪ Si se seleccionó **Contestadora automática** y se configuran múltiples Contestadoras automáticas para el sitio, seleccione la Contestadora automática deseada. ▪ Si se seleccionó **Otro número**, especifique el número en el campo **Número** exactamente como se marcaría, incluyendo cualquier código de acceso. ▪ Si se seleccionó **Anexo**, seleccione un anexo de la lista indicada en el campo **Número**. ▪ Si se seleccionó **Grupo de llamado, Grupo de envío,** o **B-ACD**, seleccione un grupo o servicio B-ACD de la lista indicada en el campo **Número**.

Grupos de contestación

Para configurar Grupos de contestación de llamadas, seleccione **Configurar** > **Telefonía** > **Grupos de telefónicos** > **Grupos de contestación** en la barra de funciones.

Visión general

Cree grupos de contestación para configurar un grupo de anexos de usuarios que puede recuperar las llamadas que suenen en los anexos que pertenecen a los miembros del mismo grupo de contestación presionando la tecla **GPickUp** del teléfono IP y la tecla *.

Se aplican las siguientes notas para usar las funciones de Contestación de llamadas en las plataformas SBCS:

- Cualquier usuario de teléfonos puede contestar una llamada presionando la tecla PickUp en su teléfono y marcando el anexo que recibe la llamada. No se necesita configuración.
- Cualquier usuario de teléfonos puede contestar una llamada que suene en un anexo del grupo de contestación usando la tecla **GPickUp** en su teléfono y marcando el anexo de contestación del grupo.
- Si el teléfono del usuario y el anexo que suena están en el mismo grupo de contestación de llamadas, el usuario de teléfono puede recuperar la llamada presionando la tecla **GPickUp** y luego la tecla *(asterisco) en su teléfono. Si sólo hay un grupo de contestación de llamadas configurado en el sistema, el usuario automática queda conectado y no tiene que presionar la tecla *.

Procedimientos

Para activar y configurar un grupo de contestación, configure los miembros como se describe a continuación, y haga clic en **Aceptar** o **Aplicar**.

Configuración	Descripción
Miembros	Defina los anexos que sean miembros del grupo de contestación. 1. Haga clic en **Miembros** para mostrar la lista de anexos Disponibles y Seleccionado en la parte inferior de la ventana Grupos de contestación. 2. Utilice los botones **Agregar** y **Eliminar** o el botón **Seleccionar todos** para desplazar a los anexos entre las listas Disponible y Seleccionado. Utilice CTRL-clic y SHIFT-clic para seleccionar múltiples anexos para desplazarlos entre las listas.

Grupos de localización

Para configurar grupos de localización, seleccione **Configurar** > **Telefonía** > **Grupos de telefónicos** > **Grupos de localización** en la barra de funciones.

La configuración del grupo de localización se describe en estas secciones:

- **Visión general, página 408**
- **Creación de un grupo de localización simple (sólo teléfonos individuales), página 408**
- **Creación de un grupo de localización combinado, página 409**
- **Edición de un grupo de localización, página 410**
- **Elimnación de un grupo de localización, página 410**
- **Vista Dependencia de grupo de localización, página 412**

Visión general

Se puede crear grupos de localización para permitir que los usuarios telefónicos transmitan anuncios a grupos de teléfonos IP de Cisco utilizando los altavoces telefónicos. Puede crear hasta 10 grupos de localización.

Sólo los teléfonos IP de Cisco pueden ser miembros de los grupos de localización.

También se puede configurar grupos de localización combinados. Un grupo de localización combinado puede contener otros grupos de localización como miembros o una combinación de teléfonos individuales y otros grupos de localización. Por ejemplo, un teléfono en una oficina inmobiliaria puede necesitar recibir llamadas que se dirigen al departamente de administración de propiedades, mientras que un teléfono diferente necesita recibir llamadas que van al departamento de ventas. Además, ambos teléfonos necesita recibir llamadas dirigidas a los empleados.

El proceso de configurar un grupo de localización combinado tiene tres pasos generales:

1. Primero, cree cada uno de los grupos de localización individuales necesarios y asígneles teléfonos.
2. Cree el grupo de localización combinado y agregue teléfonos individuales que sean miembros sólo del grupo combinado.
3. Agregue los grupos de localización combinados que se crearon en el paso 1 al grupo de localización combinado.

Un grupo de localización puede ser miembro de múltiples grupos de localización, pero un teléfono sólo puede asignarse a un solo grupo. Se admite un nivel de, colocación para los grupos de localización combinados. Consulte **Grupos de localización colocados, página 411** para ver algunos ejemplos.

Creación de un grupo de localización simple (sólo teléfonos individuales)

Para activar y configurar un grupo de localización que contenga uno o más teléfonos individuales, siga estos pasos.

PASO 1 Active la configuración para el grupo que desee crear marcando la opción **Activar**.

PASO 2 En el campo **Localización#**, especifique el anexo que se va a usar para el grupo de localización o acepte el anexo por defecto. El intervalo de anexos por defecto para los grupos de localización es de 101 a 110.

Es el anexo que se marca para llegar al grupo de llamado de localización.

PASO 3 *Opcional*. Especifique una **Descripción** que identifique a este grupo de localización. Esta descripción sólo se usa en la ventana Grupos de localización y no se muestra en los teléfonos.

PASO 4 Agregue teléfonos de miembros a la página de localización.

a. Haga clic en la ficha Teléfonos en la parte inferior de la página. La lista Disponible muestra ID del usuario y la dirección MAC para cada teléfono que no sea, actualmente, parte de un grupo de localización.

b. Haga clic en una ID de usuario en la lista **Disponible** y use los botones **Agregar** y **Eliminar** para desplazar miembros desde y hacia la lista **Seleccionados**. También puede usar los accesos directos CTRL-clic y SHIFT-clic para seleccionar múltiples teléfonos y desplazarlos entre las listas.

PASO 5 Haga clic en **Aceptar** o **Aplicar** para crear el grupo de localización.

La columna Miembros se actualiza para mostrar el número de teléfonos que son parte del grupo.

Creación de un grupo de localización combinado

Para crear un grupo de localización quecontenga otros grupos de localización, siga estos pasos.

PASO 1 Cree losl grupos de localización que desea agregar como miembros al grupo combinado e identifique los teléfonos individuales que serán parte del grupo combinado.

Consulte **Creación de un grupo de localización simple (sólo teléfonos individuales), página 408**.

PASO 2 Active la configuración del grupo combinado marcando la opción **Activar** para el nuevo grupo.

PASO 3 En el campo **Localización#**, especifique el anexo que se va a usar para el grupo de localización o acepte el anexo por defecto. El intervalo de anexos por defecto para los grupos de localización es de 101 a 110.

Es el anexo que se marca para llegar al grupo de llamado de localización.

PASO 4 *Opcional*. Especifique una descripción que identifique a este grupo de localización. Esta descripción sólo se usa en la ventana Grupos de localización y no se muestra en los teléfonos.

PASO 5 Agregue grupos de localización y teléfonos al grupo de localización.

a. Para agregar teléfonos, haga clic en la ficha Teléfonos en la parte inferior de la página. La lista Disponible muestra ID del usuario y la dirección MAC para cada teléfono que no sea, actualmente, parte de un grupo de localización.

   Haga clic en una ID de usuario en la lista Disponible y use los botones **Agregar** y **Eliminar** para desplazar miembros desde y hacia la lista Seleccionados.

b. Para agregar grupos de localización como miembros, haga clic en la ficha **Grupos** en la parte inferior de la página. Seleccione un grupo de la lista Disponibles y use los botones **Agregar** y **Eliminar** para desplazar los grupos desde y hacia la lista Seleccionados.

Un grupo de localización puede ser miembro de múltiples grupos de localización, pero un teléfono sólo puede asignarse a un solo grupo.

También puede usar los accesos directos CTRL-clic y SHIFT-clic para seleccionar múltiples teléfonos o grupos.

La columna Miembros se actualiza para reflejar el número de teléfonos y grupos de localización que son parte del grupo.

PASO 6 *Opcional*. Para ver las dependencias entre los grupos o verificar problemas de configuración en grupos de localización combinados, haga clic en **Mostrar dependencia de grupos**. Consulte **Vista Dependencia de grupo de localización, página 412**.

PASO 7 Haga clic en **Aceptar** o **Aplicar**.

Edición de un grupo de localización

Para editar un grupo de localización, haga clic en el botón **Teléfonos (n) y Grupos (n)** para el grupo que desea editar.

Las fichas Teléfonos y Grupos se actualizan para mostrar los teléfonos disponibles y seleccionados y los grupos para los grupos de localización que se van a editar.

Use los botones **Agregar** y **Eliminar** para editar los miembros del grupo y haga clic en **Aceptar** o **Aplicar**.

Elimnación de un grupo de localización

Para eliminar un grupo de localización, desmarque la configuración **Activar** que corresponda al grupo que desea eliminar y haga clic en **Aceptar** o **Aplicar**.

Antes de eliminar un grupo, se puede hacer clic en **Mostrar dependencia de grupos** para ver cuáles grupos son miembros de otros grupos.

SUGERENCIA Si el grupo que se elimina es parte de un grupo de localización combinado, éste se elimina automáticamente de este grupo. En este caso, es posible que desee actualizar la Descripción que especificó para el grupo de localización combinado para reflejar el cambio.

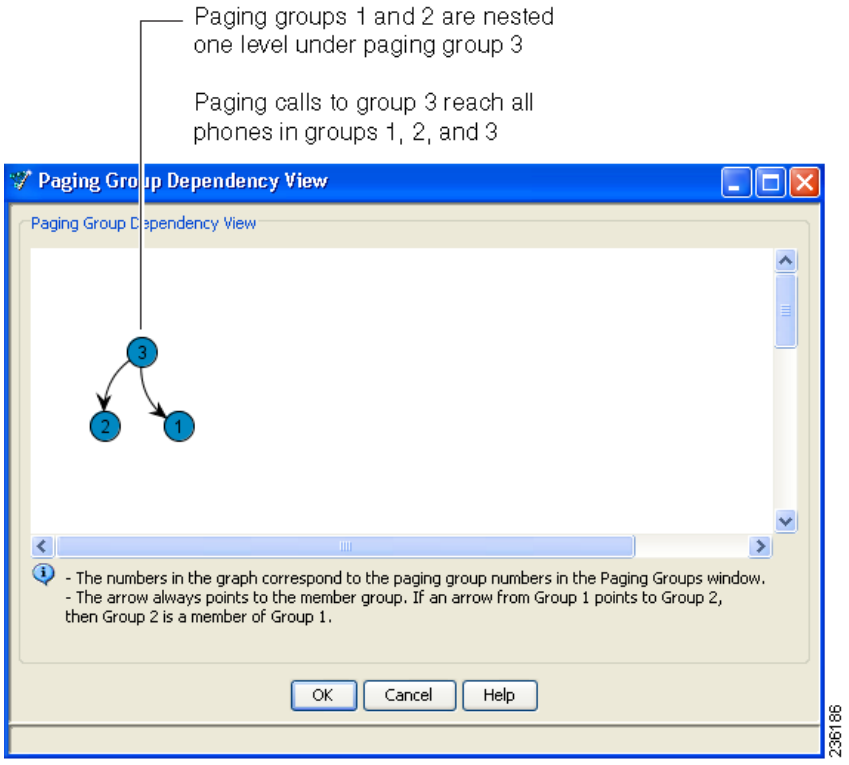
Grupos de localización colocados

Combined ("nested") paging groups are supported up to one level deep.

El siguiente escenario ilustra grupos de localización combinados con un nivel de colocación:

- Supongamos que el grupo de localización 1 contiene sólo teléfonos, el grupo de localización 2 contiene sólo teléfonos y el grupo de localización 3 contiene a los grupos de localización 1 y 2 y algunos teléfonos. En este escenario, hay un nivel de colocación.
- Una llamada al grupo 3 llega a todos los teléfonos de los grupos 1, 2 y 3.

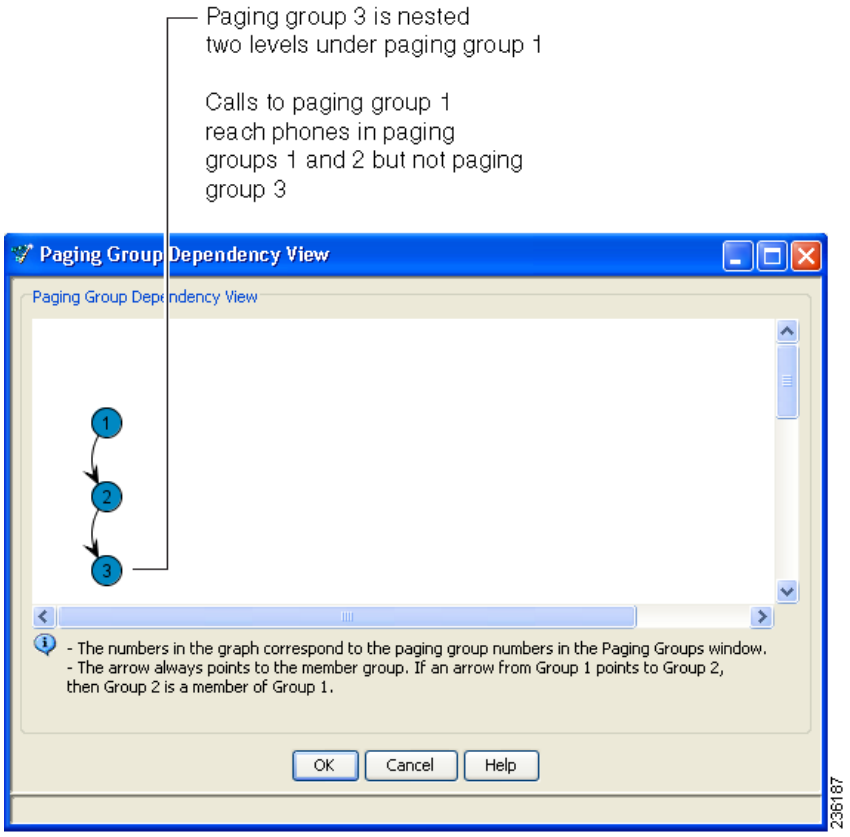
A continuación se muestra la vista de dependencia del grupo de localización para este escenario.



El siguiente escenario ilustra grupos de localización combinados con dos niveles de colocación:

- Supongamos que el grupo de localización 1 contiene al grupo de localización 2 y el grupo de localización 2 contiene al grupo de localización 3. En este escenario, hay dos niveles de colocación.
- Una llamada al grupo 1 llega a todos los teléfonos de los grupos 1 y 2, pero no llega a los teléfonos del grupo 3.

A continuación se muestra la vista de dependencia del grupo de localización para este escenario.



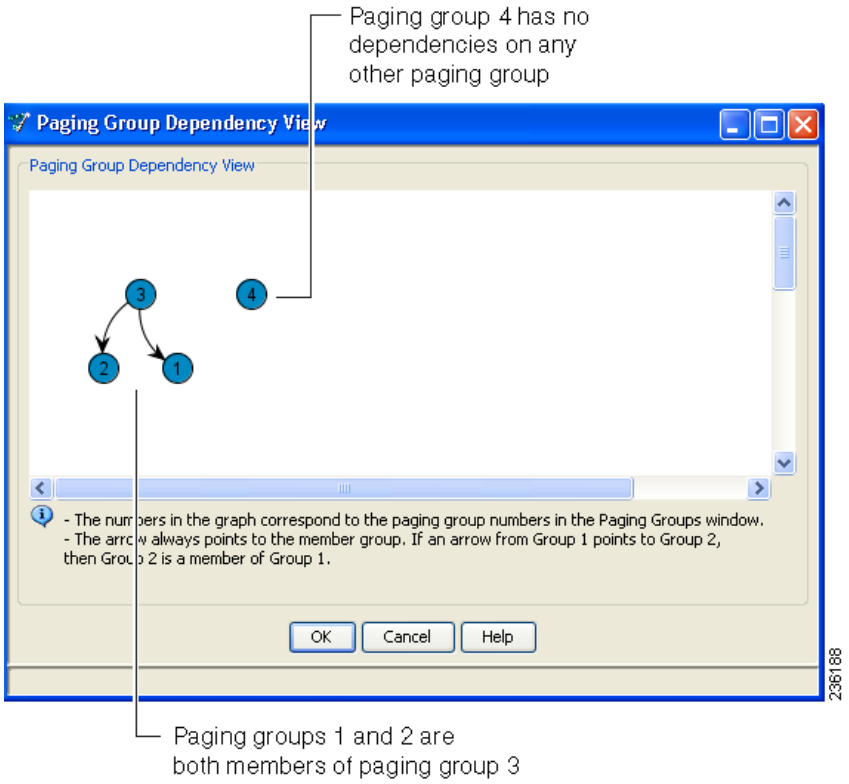
Vista Dependencia de grupo de localización

Aparece la ventana Dependencia de grupo de localización cuando se hace clic en **Mostrar dependencia de grupos** en la ventana Grupo de localización (**Configurar** > **Telefonía** > **Grupos de teléfonos** > **Grupos de localización**).

Esta ventana muestra un gráfico que puede ayduarle a ver rápidamente cuáles grupos de localización son miembros de otros grupos de localización. A continuación se muestra un ejemplo:

- Los números en la vista corresponden al número del grupo de localizació indicado en la ventana Grupos de localización.
- Las flechas en la pantalla indican cuáles grupos son miembros de otros grupos. La flecha siempre apunta al grupo miembro.

A continuación se muestran algunos gráficos de vistas de dependencia de grupos de localización como ejemplos.



13

Funciones de voz

Los temas de esta sección entregan instrucciones para configurar estas funciones de voz:

- **Parqueo de llamadas**
- **Conferencia**
- **Conference Barge**
- **Música en espera (MoH)**

IMPORTANTE Debe estar activado el acceso a Telnet para poder configurar las funciones de voz.

Parqueo de llamadas

Para configurar el parqueo de llamadas, seleccione **Configurar** > **Telefonía** > **Funciones de voz** > **Parqueo de voz** en la barra de funciones.

Visión general

El Parqueo de llamadas entrega ubicaciones de retención temporal para las llamadas entrantes. Cuando se parquea una llamada, se transfiere al anexo de parqueo de llamdas y déjela en espera hasta que se recupere por parte de otro empleado. Aparece el mensaje *<anexo de parqueo de llamadas>* de Parqueo de llamadas en el teléfono que parqueó la llamada. Para recuperar una llamada parqueada, otros usuarios pueden marcar el anexo de la ranura de parqueo.

- Se produce un campanilleo recordatorio de 1 segundo en el intervalo de recordatorio especificado y vuelve a aparecer el mensaje *<"Anexo>* de parqueo de llamadas" en la pantalla LCD del teléfono que parqueó la llamada. El mensaje y el campanilleo de recordatorio sólo se envían al teléfono que parqueó la llamada.
- Se puede seleccionar la activación de la configuración de Límite de tiempo y llamada repetida para especificar las acciones que se tomarán cuando se llegue al límite de tiempo del parqueo de llamadas. El límite de tiempo del

parqueo de llamadas es igual al número de entradas multiplicado por el número de segundos en el intervalo de recordatorio). La llamada puede transferirse al anexo que parqueó la llamada, a otro anexo o desconectarse.

Cuando se ha activado Límite de tiempo y llamada repetida, también se puede configurar el número de intervalos, el intervalo del recordatorio, el retraso de los reintentos y el número de éstos. Luego que expire el límite de tiempo, se ejecuta la acción del límite de tiempo del parqueo de llamadas.

Limitaciones y pautas

Se aplican las siguientes limitaciones y pautas al parqueo de llamadas:

- Sólo una llamada puede parquearse en cada anexo con ranura de parqueo de llamadas.
- Los teléfonos sin teclas no pueden usarse para parquear llamadas.

Procedimientos

Para crear una nueva ranura de parqueo de llamadas, haga clic en **Crear**, complete la configuración como se describe en la sección **Creación o edición de una ranura de parqueo de llamadas, página 417**. En la ventana Parqueo de llamadas, haga clic en **Aceptar** o en **Aplicar** para enviar la configuración al UC500.

Para editar una ranura de parqueo de llamadas, haga clic en una ranura de parqueo de llamadas de la lista para seleccionarla, haga clic en **Modificar** y edite la configuración como se describe en la sección **Creación o edición de una ranura de parqueo de llamadas, página 417**. En la ventana Parqueo de llamadas, haga clic en **Aceptar** o en **Aplicar** para enviar la configuración al UC500.

Para eliminar una ranura de parqueo de llamadas, haga clic en una ranura de parqueo de llamadas de la lista para seleccionarla, haga clic en **Eliminar** y seleccione **Aceptar** cuando se le pida confirmar la eliminación. En la ventana Parqueo de llamadas, haga clic en **Aceptar** o en **Aplicar** para enviar la configuración al UC500.

Creación o edición de una ranura de parqueo de llamadas

Para crear o modificar una ranura de parqueo de llamadas, siga estos pasos:

PASO 1 En el campo **Anexo**, escriba el anexo que se usará para esta ranura de parqueo de llamadas.

PASO 2 En el campo **Etiqueta de ranura** para cada nuevo anexo de ranura de parqueo, especifique una descripción para cada una de las ranuras.

PASO 3 Si es necesario, marque la opción **Activar límite de tiempo y llamada repetida**para activar la función de límite de tiempo de parqueo de llamadas y llamada repetida.

PASO 4 Si se marca **Activar límite de tiempo y llamada repetida** , realice esta configuración.

Configuración	Descripción
Intervalo de recordatorio (seg.)	Número de segundos que se esperará entre recordatorios de parqueo de llamadas. El intervalo del recordatorio por defecto es de 120 segundos.
Número de recordatorios	Número de recordatorios de parqueo de llamadas que se enviarán al teléfono que parqueó la llamada. El número por defecto es 2. El límite de tiempo del parqueo de llamadas es el número de entradas multiplicado por el número de segundos en el intervalo de recordatorio. Por ejemplo, si se configura el intervalo del recordatorio en 20 segundos y el número de reintentos es 3, una llamada puede estar parqueada hasta 60 segundos antes que expire el límite de tiempo y se tomen las acciones de vencimiento del límite de tiempo.
Cuando expira el límite de tiempo	Especifique la acción que se tomará luego que expire el límite de tiempo de parqueo de llamadas. Seleccione una de las siguientes opciones: ▪ **Volver a llamar al anexo que parqueó la llamada** (esto es por defecto). ▪ **Transferencia a anexo** Si se selecciona esta opción, escriba el **Anexo de transferencia,** configure el **Retraso de reintentos** y especifique el **Número de reintentos**. ▪ **Desconectar llamada**.
Anexo de transferencia	Si se configura la acción de expiración del límite de tiempo es **Transferencia a anexo**, escriba el anexo aquí (por ejemplo, se podría escribir un número piloto de grupo de búsqueda fo algún otro anexo).
Retraso de reintentos (segundos)	Escriba el número de segundos que se esperará entre los intentos de transferir la llamada parqueada. El número de intentos se especifica en la configuración del **Número de reintentos**. El retraso de reintentos por defecto es de 120 segundos.

Configuración	Descripción
Número de reintentos	Escriba el número de reintentos que se permitirán al transferir una llamada parqueada. El número de reintentos por defecto es 2.

PASO 5 Haga clic en **Aceptar**.

Conferencia

Para configurar una conferencia multipartita, seleccione **Configurar** > **Telefonía** > **Funciones de voz** > **Conferencias** en la barra de funciones.

Para obtener más información sobre la configuración de conferencias, consulte estos temas:

- **Visión general, página 419**
- **Activación y configuración de conferencias multipartitas (MeetMe y Ad Hoc), página 421**
- **Limitaciones y notas que se aplican a las conferencias multi-partitas., página 422**
- **Conference Barge, página 422**

Visión general

En la ventana Conferencia, se puede seleccionar si se activa la conferencia multi-partita y configurar las opciones de conferencia.

NOTA La conferencia multi-partita debe activarse para poder usar las funciones Conference Barge (cBarge) y Privacidad.

Cuando se desactiva la conferencia multi-partita:

- Los recursos del software se usan para las conferencias.
- Se puede especificar el orden máximo de sesiones de llamadas simultáneas tripartitas que se permitirá en el sistema.

Cuando se activa la conferencia multi-partita:

- Se usan recursos de hardware (DSP).

  Configuration Assistant detecta automáticamente la plataform UC500 que se están configurando y determina el número máximo de participantes admitidos por conferencia y sesiones simultáneas de conferencias que pueden configurarse tanto para las conferencias Meet-Me y Ad Hoc.

  Las plataformas UC500 de Cisco que admiten 24 o más usuarios tienen aproximadamente el doble de recursos de conferencia de hardware y puede admitir un mayor número de participantes y sesiones.

  NOTA Las conferencias por hardware están desactivadas si no hay suficientes recursos de hardware. Por ejemplo, puede desactivarse las conferencias de hardware si se agrega una tarjeta T1/E1 adicional a un chasis de UC500-16U, porque los puertos de voz consumen recursos del mismo conjunto de recursos asignado a las conferencias de hardware.

- Se puede configurar tanto las conferencias MeetMe y Ad Hoc.
  - Una *conferencia Ad Hoc* es un tipo de conferencia en la que una parte llama a otra y cualquiera de ellas decide agregar a un tercero a la llamada.
  - Una *conferencia MeetMe* es aquella en la que las partes marcas un número de conferencia MeetMe determinado previamente.

    El creador de la conferencia levanta el auricular, presiona la tecla **MeetMe** en su teléfono, escucha un tono de confirmación y marca el número de MeetMe. Una vez que se inicia la conferencia, otras partes se unen a la conferencia MeetME marcando el mismo número MeetMe.

    Cuando se configure la conferencia MeetME, todos los usuarios telefónicos tienen permiso para iniciar conferencias MeetMe. El creador de la conferencia MeetMe puede presionar la tecla **ConfList** para mostrar a todos los participantes, la tecla **RmLstC** para quitar al último que se ha unido, y para quitar a un participante de la conferencia.

    Las teclas de conferencias MeetMe se configuran y se aplican a los teléfonos automáticamente cuando se activa la función de conferencias multipartitas y se configuran los anexos de MeetMe.

- Se puede activar o desactivar la reproducción de tonos cuando quien llama se une o abandona una conferencia multi-partita. Por defecto, quedan desactivados.

Activación y configuración de conferencias multipartitas (MeetMe y Ad Hoc)

Para activar y configurar conferencias multipartitas, siga estos pasos:

PASO 1 En la ventana Conferencias, seleccione si se activan las conferencias multipartitias.

- Marque la casilla **Activar conferencias multipartitias** para activar las conferencias multipartitias (usa recursos de hardware).
  - Cuando se selecciona esta opción, puede configurarse tanto la conferencia Ad Hoc omo MeetMe.
  - El número máximo de sesiones que puede configurarse depende del número de recursos de hardware para la plataforma UC500 que se está configurando.
- Si no se selecciona la activación de conferencias multipartitas, use el menú desplegable **Máximo de sesiones de llamadas tripartitas** para configurar el número máximo de sesiones de conferencias Ad Hoc tripartitas simultáneas que se desee permitir.
  - Cuando se selecciona esta opción, los recursos de software en IOS de Cisco se usan para la conferencia. No son necesarios los recursos de hardware. Esta opción se usa cuando se desactiva o no se configura la conferencia por hardware.
  - Cada conferencia Ad Hoc puede tener hasta 3 participantes.

PASO 2 Si se marca **Activar las conferencias multipartitas**, realice la siguiente configuración.

a. Seleccione un **Modo**, ya sea G711 (modo individual) o G711/G729 (modo mixto).

   La configuración **Modo** determina la cantidad de recursos de conferencia de hardware necesarios para cada llamada. G711 utiliza menos recursos que G711/G729.

El modo sólo G711 se recomienda para las implementaciones donde sólo se utilizan enlaces locales. El modo mixto (G711/G729) se recomienda para las implementaciones que incluyen enlaces SIP, si el Proveedor de servicio SIP admite G729.

b. En **Configuración de tonos**, seleccione si se activa o desactiva la reproducción de tonos cuando quien llame se une o abandona una conferencia multi-partita.

   Por defecto, los tonos de unión y abandono de conferencia están desactivados. Cuando se desaciva la conferencia multi-partita, también se desactiva la configuración de tonos.

c. Utilice el menú desplegable para seleccionar el **Máximo de participantes** por conferencia.

d. Utilice la barra deslizante a la derecha del menú **Sesiones** para asignar sesiones entre las conferencias Ad Hoc y Meet-Me. El número total de sesiones debe ser igual o menor que el máximo de sesiones simultáneas.

e. Edite los números de anexos Meet-Me o deje los valores por defecto.

PASO 3 Haga clic en **Aceptar** o **Aplicar**.

Limitaciones y notas que se aplican a las conferencias multi-partitas.

- Si se está configurando un sistema con 8 ó 16 usuarios con una VIC y ya se han configurado conferencias Ad Hoc basadas en hardware en el dispositivo, antes de configurar cualquiera tarjeta VIC desde CCA, debe restaurarse las conferencias Ad Hoc al modo basado en software desmarcando **Activar conferencias multipartitas** y haciendo clic en **Aplicar**.
- Si existe alguna configuración fuera de banda relacionada con DSP (por ejemplo, Transcoding), no está disponible la función de conferencias. Se debe quitar la configuración fuera de banda existente o siga configurándola fuera de ella.

Conference Barge

Para configurar Conference Barge (cBarge) y un botón de Privacidad opcional para los teléfonos cBarge phones, seleccione **Configurar** > **Telefonía** > **Funciones de voz** > **Conference Barge** en la barra de funciones.

IMPORTANTE La función de conferencias multi-partitas debe estar activada antes de poder configurar las funciones cBarge y Privacidad. Sólo puede configurarse Conference Barge en teléfonos OP que tengan al menos un anexo compartido de ocho líneas.

Para obtener información acerca de las funciones cBarge y Privacidad, consulte los siguientes temas.

- **Descripciones de las funciones Conference Barge y Privacidad, página 423**
- **Uso de cBarge y de Privacidad y ejemplos**
- **Requisitos previos para cBarge y Privacidad, página 426**
- **Teléfonos no admitidos, página 427**
- **Configuración de anexos compartidos de líneas octales, página 427**
- **Configuración de funcioens Conference Barge y Privacidad, página 428**
- **Eliminación de cBarge y Privacy del teléfono de un usuario, página 428**

Descripciones de las funciones Conference Barge y Privacidad

La función cBarge permite que los usuarios con ocho líneas compartidas en sus teléfonos presionen la tecla **cBarge** para “subirse” y unirse a una llamada en progreso en esa línea compratida. Cuando un tercero se une a la llamada, se crea una conferencia Ad Hoc. Otros usuarios también que también tengan cBarge configurada para la misma línea compartida pueden unirse a la conferencia, hasta llegar al número máximo de participantes. Estas pautas se aplican a la función cBarge:

- **Máximo de sesiones cBarge**. Número máximo de sesiones activas de conferencias cBarge es igual que el número máximo de sesiones de conferencias Ad Hoc permitidas en su sistema. Puede ver esta información en la ficha Conferencia.
- **Número máximo de participantes cBarge por sesión**. Una conferencia cBarge admite el número máximo de participantes que esté configurado para las conferencias Ad Hoc en su plataforma UC500. Puede ver esta información en la ficha Conferencia.
- Si no hay una sesión de conferencias Ad Hoc disponible, o se llega al número máximo de participantes, la solicitud de cBarge se rechaza y se muestra un mensaje de error en el teléfono de inicio.

- Cuando un particpantes abandona la llamada, ésta sigue siendo una llamada de conferencia si permanecen, al menos, tres (3) participantes en la línea. So sólo dos participantes siguen en la conferencia, ellos se reconectan como una llamada de punto a punto, lo que libera los recursos del puente de conferencias.
- Cuando el participante al que se llama parquea la llamada o se una a la llamada por medio de otra llamada, el iniciador de cBrage y los otros participantes permanecen conectados.

La función Privacidad funciona en conjunto con cBarge. Esta fnción permite que los usuarios con cBarge activada para un anexo compartido bloqueen usuarios que no comparten el anexo y no puedan ver la información de la llamada ni reanudar una llamada ni subirse a una llamada en el anexo compartido. El teléfono debe tener un botón de línea disponible para activar esta función.

Cuando se configura Privacidad para un teléfono con cBrage usando CCA:

- Se ubican un teléfono de Privacidad en el teléfono. Si no hay un botón de línea disponible, aparece un mensaje en la barra de errores de CCA.
- El usuario del teléfono puede presionar el botón Privacidad en su teléfono para activar o desactivar la función Privacidad.
- Cuando Privacidad está activada, el botón de Privacidad en el teléfono del usuario luces ámbar.

Uso de cBarge y de Privacidad y ejemplos

Uso. Supngamos que el Usuario A y el Usuario B tienen asignado el anexo 222 a un botón en sus respectivos teléfonos. El anexo 222 está configurado como un anexo compartido de líneas octales. La funcnión cBarge se activa para el anexo 222 en ambos teléfonos y la función Privacidad se desactiva (Off) en ambos teléfonos.

La tecla **cBarge** queda disponible cuando el Usuario A presiona el botón de línea para que el anexo 222 conteste una llamada entrante en la línea compartida. Mientras el Usuario A esté con la llamada en el anexo 222, el Usuario B puede presionar la tecla **cBarge** en su teléfono para unirse a la conversación con el Usuario A y el otro participantes en el anexo 222. Esto se logra internamente al crear una conferencia Ad Hoc entre el Usuario A, el Usuario B y el otro participzante en el anexo 222.

Para extender este ejemplo:

- Si un tercer participante, el Usuario C tiene el anexo de líneas octales compartido configurado en su teléfono, también puede presionar la tecla **cBarge** en su teléfono para unirse a la conferencia.
- Luego, si el Usuario A presiona el botón Privacidad en su teléfono para activar esa función, la tecla **cBarge** no está disponible para los otros usuarios con el anexo 222 en sus teléfonos y ningún otro usuario puede unirse a la llamada.

cBarge y Privacidad pueden activarse o desactivarse en los teléfonos que comparten el misno anexo de líneas octales. Cuando se desactiva cBarge, puede desactivarse la función Privacidad. A continuación se encuentran algunos ejemplos.

Ejemplo 1. En un entorno de trabajo donde los empleados son pares, todos los teléfonos que comparten el mismo anexo compartido de 8 líneas tienen tanto a cBarge como Privacidad activadas.

Teléfonos/ Usuarios	cBarge	Privacidad	Resultado de la configuración
Todos los teléfonos	Activados	Activados	Caulquier usuario del anexo compartido puede subirse a cualquier llamada en dicho anexo y/o establecer Privacidad para las llamadas en el anexo compartido.

Ejemplo 2. En un entorno de un pequeño centro de llamados, donde un supervisor y múltiples empleados comparten el mismo anexo de líneas octales, cBarge y Privacidad pueden configurarse como se indica a continuación.

Teléfonos/ Usuarios	cBarge	Privacidad	Resultado de la configuración
Teléfono del supervisor	Activados	Desactivado	El supervisor puede entrar en ninguna de las llamadas de sus empleados sobre la ampliación compartida octal línea. No hay necesidad de activar Privacidad en el teléfono del supervisor, ya que ninguno de los empleados puede subirse a una llamada en el anexo compartido.

Teléfonos/ Usuarios	cBarge	Privacidad	Resultado de la configuración
Teléfonos de empleados	Desactivado	Desactivado	Los empleados con este anexo de líneas octales compartido no pueden subirse en niguna llamada ni activar la Privacidad para llamadas en este anexo.

Ejemplo 3. En una oficina donde un administrador tiene a varios supervisores que controlan un pequeño grupo de empleados, se puede configurar cBarge y Privacidad como se indica a continuación.

Teléfonos/ Usuarios	cBarge	Privacidad	Resultado de la configuración
Teléfono del administrador	Activados	Activados	El administrador puede subirse a llamadas en el anexo compartido realizadas por supervisores o empleados. Sólo el administrador puede hacer llamadas privadas en este anexo.
Teléfonos de supervisores	Activados	Desactivado	El supervisor puede entrar en ninguna de las llamadas de sus empleados sobre la ampliación compartida octal-línea, pero no es posible entrar en una llamada en la extensión para compartir, cuando el Administrador de Privacidad ha activado.
Teléfonos de empleados	Desactivado	Desactivado	Los empleados con este anexo de líneas octales compartido no pueden subirse en niguna llamada ni activar la Privacidad para llamadas en el anexo compartido.

Requisitos previos para cBarge y Privacidad

Para configurar las funciones Conference Barge y Privacidad, su sistema debe cumplir con los siguientes requisitos:

- Se necesita el paquete de software 7.0.2 ó posterior para el UC500 para asegurar que las versioens necesarias de IOS y CUE de Cisco estén instaladas (IOS 12.4(20)T2 ó posterior y CUE 7.0 ó posterior). Para los teléfonos 7931 de Cisco, se necesita el paquete de software 8.0.4 para UC500.

- Debe activarse la conferencia multi-partita y debe configurarse las sesiones y participantes de las conferencias Ad Hoc antes de poder configurar las funciones cBarge y Privacidad. Consulte **Conferencia, página 419**.
- Deben configurarse los anexos compartidos de líneas octales antes de poder configurar las funciones cBarge y Privacidad. Consulte **Configuración de anexos compartidos de líneas octales, página 427**.

Teléfonos no admitidos

Las fnciones cBarge y Privacidad no pueden configurarse para teléfonos con un solo botón y para los que no admitan números de directorio compartido (DN) de líneas octales. Los teléfonos que no admiten DN de líneas octales se indican a continuación:

- Teléfonos FXS análogos
- ATA
- Teléfonos modelos 7935,7936,7937 y 39xx de Cisco
  Los teléfonos modelos 7931 *sí* se admiten.
- Teléfonos IP Modelo CP-521 de Cisco
- Teléfonos IP Modelo CP-52xG de Cisco
- Teléfonos IP Modelos 7902, 7905, 7906, 7910, 7911, 7912 , 7920 y 7985 de Cisco
- Todos los teléfonos de la serie SPA500 de Cisco (Modelos SPA501G, SPA525G, SPA525G2 y SPA50x)
- Todos los teléfonos IP de Cisco serie SPA300
- Teléfonos analógicos SCCP (tipo VG224)

Configuración de anexos compartidos de líneas octales

Para obtener mayor información sobre las líneas octales, consulte **Líneas octales, página 375**.

Para configurar un anexo compartido de líneas octales en un teléfono para que **cBarge** se active en un teléfono, siga estos pasos.

PASO 1 Siga las instrucciones de esta sección **Anexo compartido, página 363**.

PASO 2 Asegúrese que el tipo de línea se configura como **Línea octal** al configurar las opciones de línea para el botón de línea compartido en el teléfono.

PASO 3 Una vez que se ha creado el anexo de línea octal compartido, agregue la línea compartida a un botón en cada uno de los teléfonos que se configurará con cBarge y Privacidad activada.

Para ver una lista de teléfonos que no admiten esta función, consulte **Teléfonos no admitidos, página 427**.

PASO 4 Haga clic en **Aceptar** para aplicar los cambios y cerrar la ventana Usuarios y teléfonos.

Configuración de funcioens Conference Barge y Privacidad

Una vez que se haya activado la conferencia multi-partita y se haya configurado los necesarios anexos compartidos de líneas octales en los teléfonos, siga estos pasos para configurar las funciones cBarge y Privacidad para estos anexos.

PASO 1 En la barra de funciones, seleccione **Configurar** > **Telefonía** > **Funciones de voz** > **Conference Barge**.

Se indican todos los teléfonos del sistema con anexos compartidos de líneas octales. Las funciones cBarge y Privacidad están desactivadas en estos anexos por defecto.

PASO 2 Para cada teléfono, seleccione si se activará cBarge y Privacidad.

cBarge y Privacidad pueden activarse o desactivarse en los teléfonos que comparten el misno anexo de líneas octales. Para ver algunos ejemplos de uso, consulte **Uso de cBarge y de Privacidad y ejemplos, página 424**.

Para activar Privacidad para una línea octal compartida, se debe tener disponible un botón de línea. Si no hay botones de línea disponibles en el teléfono, la barra de errores muestra el mensaje “No se puede activar Privacidad en <*Nombre Apellido*> (*nombre de usuario*) porque no hay botones de línea disponibles.”

PASO 3 Haga clic en **Aceptar** o **Aplicar**.

Eliminación de cBarge y Privacy del teléfono de un usuario

Para eliminar cBarge o Privacidad de un teléfono, siga estos pasos.

PASO 1 En la barra de funciones, seleccione **Configurar** > **Telefonía** > **Funciones de voz** > **Conference Barge**.

PASO 2 Ubique a un usuario de la lista.

PASO 3 Para eliminar a cBarge del teléfono asociado al usuario, seleccione **Desactivado** de la lista desplegable en la columna cBarge.

PASO 4 Para eliminar a Privacidad del teléfono asociado al usuario, seleccione **Desactivado** de la lista desplegable en la columna Privacidad.

PASO 5 Haga clic en **Aceptar** o **Aplicar**.

Música en espera (MoH)

Para configurar Música en espera, seleccione **Configurar** > **Telefonía** > **Funciones de voz** > **Música en espera** en la barra de funciones.

Visión general

Música en espera (MOH) entrega música desde una fuente externa o archivo .WAV en la memoria flash del UC500 a quien llame y que haya sido dejado en espera por parte de un tercero.

Procedimientos

Para configurar la música en espera, siga estos pasos:

PASO 1 En el campo **Archivo de audio**, seleccione **Ninguno** o seleccione un archivo de audio.

PASO 2 Seleccione si se activa la música en espera para las llamadas internas y/o active la entrada Música en espera desde una fuente conectada al puerto externo Música en espera del UC500.

- Cuando se marca**Activar música en espera para llamadas internas**,las llamadas entre teléfonos IP internos que se dejan en espera escuchan música. De lo contrario, las llamadas internas escuchasn el tono de espera.
- Cuando se marca **Activar música externa en puerto de espera**, se activa automáticamente la música en espera para las llamadas internas y no puede desactivarse. Si se selecciona un archivo de audio y el puerto externo en espera también se activa, la entrada de música desde el puerto externo tiene preferencia. El archivo de audio seleccionado sirve como fuente de música de respaldo en caso que la fuente externa falle o no esté disponible.

- Siempre está activado MoH para un enlace PSTN o SIP, incluso si está desactivado MoH para las llamadas internas. Para desactivar MoH para las llamadas de enlaces PSTN o SIP, demarque todas las opciones y seleccione Ninguno para el archivo de audio.

PASO 3 Haga clic en **Aplicar**.

Para cargar un archivo de audio personalizado para Música en espera (archivo .AU) en el UC500:

PASO 1 Seleccione **Inicio** > **Topología** para mostrar la vista Topología.

PASO 2 Arrastre y suelte el archivo de audio desde su escritorio al icono del UC500 en la vista Toplogía.

El archivo d audio debe tener una extensión .AU.

Una vez que se haya cargado el archivo, queda disponible en la lista de selección Archivo de audio para Música en espera.

Para obtener especificaciones e instrucciones sobre cómo crear un archivo de audio personalizados para Música en espera, consulte la *Guía del administrador de sistema de Unified Communication Manager Express de Cisco*, disponible en Cisco.com.

14

Gestión de llamadas

Se analizan los siguientes temas:

- **Calendarios**
- **Contestadora automática**
- **Distribución básica automática de llamadas (ACD)**
- **Atención nocturna**
- **Grabación en vivo**
- **T.37 Facsímil a correo**

Calendarios

Para configurar calendarios, seleccione **Configurar** > **Telefonía** > **Gestión de llamadas**> **Calendarios**.

Los horarios de trabajo, festivos y calendarios de atención nocturna se administran en estas fichas de la ventana Calendarios:

- **Horario de trabajo**
- **Festivos**
- **Atención nocturna**

Horario de trabajo

El calendario Horario de trabajo define el horario de apertura y cierre. Ello activa a la **Contestadora automática** para que se configure y presente diferentes solicitudes y realice diferentes acciones para las horas de apertura y cierre. Se puede definir hasta cuatro diferentes calendarios de trabajo.

Si se utilizan múltiples contestadoras automáticas, se puede definir un calendario separado para cada una. Se puede configurar un horario de apertura y cierre para cada día de la semana, en incrementos de media hora.

Para activar y definir un calendario:

PASO 1 Seleccione un calendario desde la lista al lado izquierdo de la ficha.

PASO 2 Haga clic en **Activar Horario de trabajo** para activar y abrir el calendario seleccionado para editarlo:

PASO 3 Edite el nombre del calendario para entregar un nombre más descriptivo. El nombre por defecto es systemschedule.

PASO 4 Utilice los menús desplegables de la parte superior de la ventana para especificar el horario de apertura y cierre para los días de la semana, luego haga clic en **Actualizar Tabla** para actualizar la pantalla.

También se puede hacer clic en las casillas de verificación dentro de la tabla para definir el horario de trabajo.

Las ranuras de tiempo marcadas indican las horas en que el negocio está abierto.

PASO 5 Haga clic en **Aceptar** o **Aplicar**.

Festivos

Hasta 26 festivos pueden definirse por cada año, para el año actual y para el próximo. Sin embargo, si también se configura el atención nocturna, éste sólo se activa durante los primeros 15 días festivos especificados (se muestra un mensaje de advertencia si se activa el atención nocturna y se agregan más de 15 días festivos). En los festivos calendarizados, la **Contestadora automática** activa sus solicitudes y acciones del Horario de cierre. Se activa **Atención nocturna**, si es que está configurado para este sitio.

También se puede modificar o eliminar festivos o copiarlos todos desde el año actual hacia el próximo. Al copiar festivos del año actual hacia el próximo, si la misma fecha aparece en ambos años, se utiliza la entrada del año actual.

NOTA No se puede modificar el año para un festivo existente. Elimine o vuelva a agregar el festivo si se necesita cambiar el año.

Para agregar un festivo:

PASO 1 En la ventana Calendario, seleccione el año actual o el próximo.

PASO 2 Haga clic en **Agregar** para abrir la ventana Agregar festivo (consulte **Agregar festivo, página 433**).

PASO 3 Cuando se termine de agregar los festivos, haga clic en **Aceptar**.

Agregar festivo

Esta ventana aparece cuando se hace clic en **Agregar festivos** en la ventana Calendario.

Para agregar un festivo, siga estos pasos:

PASO 1 Haga clic en el icono del calendario y seleccione una fecha del año seleccionado.

PASO 2 Utilice las flecha adelante (>) y atrás (<) para ir a los diferentes meses del calendario.

PASO 3 Ingrese una descripción para el festivo. La descripción puede contener hasta 64 caracteres.

PASO 4 Haga clic en **Aceptar**.

Atención nocturna

Especifique el horario en que se activa el Atención nocturna para cada día de la semana.

Una vez que se haya configurado un calendario de atención nocturna, vaya a **Configurar** > **Telefonía** > **Gestión de llamadas**> **Atención nocturna** para activar y configurar esta función.

Durante el horario de Atención nocturna:

- El Atención nocturna se activa para los teléfonos y anexos especificados.
- Las llamadas a anexos con desvío de llamada a otro número despúes de la hora de cierre se desvían automáticamente a ese número.

En los festivos, se activa el Atención nocturna si está configurado para este sitio.

Para configurar el horario del Atención nocturna, siga estos pasos:

PASO 1 Seleccione un día de la semana del menú desplegable o haga clic en la fila correspondiente al día de la semana en la pantalla del resumen del Calendario de atención nocturna.

PASO 2 Utilice los menús desplegable **desde** y **hasta** para definir las horas para el día seleccionado. Haga clic en **Eliminar** para borrar las horas de ese día.

PASO 3 Haga clic en **Agregar** para agregar horas. Pase por alto este paso si está eliminando horas.

PASO 4 Siga seleccionando días de la semana y configurando las horas del Atención nocturna.

Utilice la opción **Copiar fila seleccionada a** para copiar la configuración de un día a otro diferente, a otros días de la semana o del fin de semana.

Ejemplo: Si se desea que el Atención nocturna esté activo entre 4:00 pm y 9:00 am de Lunes a Viernes y las 24 horas los Sábados y Domingos, configure el horario Desde y el horario Hasta como se indica a continuación:

Día	Horario Desde (HH:MM)	Horario Hasta (HH:MM)
Lunes	**17:00**	**8:00**
Martes	**17:00**	**8:00**
Miércoles	**17:00**	**8:00**
Jueves	**17:00**	**8:00**
Viernes	**17:00**	**8:00**
Sábado	**9:00**	**8:00**
Domingo	**9:00**	**8:00**

PASO 5 Haga clic en **Aceptar** o **Aplicar**.

Para obtener más información, consulte estos temas:

- **Contestadora automática, página 435**
- **Atención nocturna, página 451**

Contestadora automática

Para configurar una Contestadora automática y administrar las instrucciones y comandos de ella, seleccione **Configurar** > **Telefonía** > **Gestión de llamadas**> **Contestadora automática**.

Se analizan los siguientes temas:

- **Requisitos previos**
- **Configuración de Contestadora automática**
- **Solicitar Administración**
- **Administración del archive de comandos**

Requisitos previos

Antes de configurar los saludos y la configuración de la Contestadora automática, ya deberían estar configuradas las siguientes funciones telefónicas:

NOTA Debe estar activado el acceso a Telnet para poder configurar las funciones de la contestadora automática.

- Anexos telefónicos y cuentas de correo de voz asociadas
- Plan de numeración y funciones de voz asociadas
- Horarios para las horas de trabajo normales y festivos
- Parámetros de servicio ACD básica, si se utilizan
- Prefijo de transferencia de correo de voz, si se utiliza **Transferencia directa a correo de voz** como una opción de Contestadora automática

Configuración de Contestadora automática

La ficha Contestadora automática muestra, inicialmente, las opciones para activar y desactivar la Contestadora automática y seleccionar si configurar una Contestadora automática estándar con un nivel de menús (el por defecto) o una Contestadora automática de múltiples niveles con submenús.

Para ver instrucciones sobre cómo configurar la Contestadora automática, consulte las siguientes secciones:

- **Modos de Contestadora automática, página 436**

- **Configuración de Contestadora automática en modo Estándar, página 436**
- **Configuración de Contestadora automática de múltiples niveles, página 439**

Modos de Contestadora automática

Están disponibles tres modos de Contestadora automática:

- **Apagado**. Cuando el modo de Contestadora automática se configura en **Apagado**, se utiliza la configuración de fábrica y el comando de AA se configura como aa.aef.

  Si selecciona desactivar la Contestadora automática configurando el modo en **Apagado**, se eliminan el mapeo del plan entre el número PSTN de la AA y los anexos internos de la AA. Podría ser necesario modificar la configuración de la función de voz que referencian a la Contestadora automática, como el número principal, grupos de llamado y de envío de llamadas.

- **Estándard**. El modo Contestadora automática **Estándar** le permite configurar hasta tres (3) Contestadoras automáticas, cada una con un nivel de menús individual. Consulte **Configuración de Contestadora automática en modo Estándar, página 436**.

- **Multi-nivel**. El modo **Multi-nivel** de Contestadora automática permite configurar la AA para que presente un menú principal con hasta tres (3) submenús a quien llama. Consulte **Configuración de Contestadora automática de múltiples niveles, página 439**.

Cuando se cambia el modo de la Contestadora automática, no se conserva la configuración existente de la Contestadora automática. Se deben configurar todos los parámetros si se cambia de modo.

Configuración de Contestadora automática en modo Estándar

Para configurar una Contestadora automática estándar, siga estos pasos.

PASO 1 En el campo **Modo**, asegúrese que esté seleccionado **Estándar**.

PASO 2 En **Número de contestadoras automáticas**, seleccione la cantidad de Contestadoras automáticas que se van a configurar.

PASO 3 En el campo **Anexo de AA**, especifique el número del anexo al que se tendrá acceso para las funciones generales de Contestadora automática de la empresa.

Por lo general, se trata del número de la extensión telefónica principal para las oficinas. Cuando se llame a este anexo, se ejecutará el comando de Contestadora automática. El anexo de AA debe ser único en todo el sistema. El anexo de AA por defecto es 398.

PASO 4 En el campo **Número PSTN de AA**, especifique el número PSTN al que se tendrá acceso para las funciones generales de Contestadora automática de la empresa.

El Número PSTN de AA puede comenzar con un carácter "+".

PASO 5 En el campo **Comando de AA**, seleccione el comando de AA que se ejecutará cuando se active la Contestadora automática.

Se indican los siguientes comandos del sistena y de CAA.

- **aa_sbcs_v03.aef** es el comando por defecto. Éste es un comando más avanzado que admite menús de AA de múltiples niveles y activa la configuración de acciones de teclas separadas y solicita especificar las horas de operación y de cierre, basado en los calendarios definidos previamente para días laborales y festivos. También admite opciones para **Discado por número**y **Permitir transferencia externa**, y también como reserva hacia un número configurable (**No existe la opción Transferir a:**) si quien llama no toma ninguna acción una vez que se reproduce el saludo del menú principal tres veces.
- **aa_sbcs_v02.aef** proporciona las mismas funciones que **aa_sbcs_v03.aef** excepto que no admite el campo **No existe la opción Transferir a:**
- **aa.aef** y **aasimple.aef** son los comandos por defecto del sistema que se implementan como parte de Unity Express (CUE) de Cisco. Cuando se selecciona cualquiera de estos comandos, CAA sólo permite que se configuren los parámetros base (anexo de AA, número PSTN de AA y comando de AA).
- **aa_transfer2.aef** es una versión actualizada del comando aa_transfer.aef que admite dos opciones de teclas adicionales (**#** y ***) y la acción**Reproducir saludo**.

Se puede cargar comandos personalizados definidos por el usuario. Sin embargo, para comandos definidos por el usuario, CCA sólo configura el anexo de AA y en número de PSTN de AA. Consulte **Administración del archive de comandos, página 443**. Estos pasos de configuración sólo se aplican cuando se selecciona el comando de AA **aa_sbcs_v02.aef** o **aa_sbcs_v03.aef**.

No se admite la Migración entre comandos de la AA. Si se cambia el comando de la AA, se elimina cualquier comando existente.

PASO 6 En el campo **Horario de trabajo**, seleccione el horario laboral que se utilizará para esta Contestadora automática.

PASO 7 Seleccione si se activa **Discar por número en cualquier momento** y **Permitir transferencia externa**. Cuando se activa**Discar por número en cualquier momento**, quien llama puede especificar el número de la persona a la que llama y la llamada se enviará a ese número.

PASO 8 Si se está usando el comando **aa_sbcs_v03.aef**, en forma opcional se puede especificar un número en el campo **No existe la opción Transferir a:** Este número puede ser un número PSTN externo o un anexo interno.

- Si se especifica un número PSTN externo, especifique el número exactamente como lo marcaría en el teléfono, incluyendo cualquier código de acceso.
- Si se especifica un anexo interno, asegúrese que se haya indicado el anexo correctamente. CCA no verifica si el anexo es válido en su sistema.

Si se especifica un número para **No existe la opción Transferir a:** y quien llama no presiona una tecla para la que ha definido una acción, se repite el saludo del menú principal dos veces más, y luego la llamada se redirige a dicho número.

Si no se especifica un número en este campo y quien llama no presiona una tecla para la que se ha definido una acción, se repite el saludo del menú principal dos veces más, y luego la llama se termina.

PASO 9 Configure saludos y acciones para las teclas tanto para el **Horario de trabajo** como para el **Horario fuera de trabajo**.

a. En el campo **Saludo de menú**, seleccione el archivo .wav para que se reproduzca lel saludo cuando se active la Contestadora automática.

b. (*Opcional*) Haga clic en **Grabar** para utilizar la función grabar y reproducir de CCA para grabar saludos del menú.

c. Defina las acciones de las teclas. Para cada acción de las teclas que desee definir:

- Haga clic en la columna **Modo** para seleccionar el tipo de acción.
- Haga clic en la columna **Parámetros** para definir parámetros de ingreso, si es necesario.

Por ejemplo, para hacer que AA envíe la llamada a un grupo de búsqueda cuando el usuario presione 4, seleccione **Llamar a grupo de búsqueda** en la columna **Modo**, luego seleccione un grupo de búsqueda de la lista de grupos de llamado disponibles que se indican en la columna **Parámetro**.

Las acciones disponibles incluyen **Llamar a grupo de envío**, **Llamar a grupo de búsqueda**, **Llamar a correo de voz**, **Transferir a correo de voz**, **Transferir a ACD básica**, **Llamar a anexo**, **Reproducir saludo**, **Discar por nombre**, **Discar por número**, **Llamar a otro número**, y **Ninguna**.

Si se especifica un número externo para **Llamar a otro número**, asegúrese que éste se especifique exactamente como se debe discar, incluyendo códigos de acceso o de larga distancia, si son necesarios.

PASO 10 Haga clic en **Aceptar** o **Aplicar**.

Configuración de Contestadora automática de múltiples niveles

El modo **Multi-nivel** de Contestadora automática permite configurar la AA para que presente un menú principal con hasta tres (3) submenús a quien llama.

Si selecciona tener múltiples Contestadoras automáticas (pueden definirse hasta 3), se muestran fichas adicionales para configurar cada Contestadora automática y se aplicana los mismos pasos de configuración.

Configurar una AA de múltiples niveles con submenús es similar a configurar una Contestadora automática **estándar**, con estas opciones:

- Para la configuración del menú Principal, siempre se utiliza el comando por defecto para la Contestadora automática (**aa_sbcs_v02.aef**) y no se muestra la opción de selección de comandos.
- Para los submenús, siempre se utiliza el comando aa_transfer2.aef, y no se muestra la opción de selección de comandos.
- Se entrega una acción de teclas adicional, **Llamar menú**, para que se pueda asignar teclas para la navegación entre el menú principal y los submenús.

Para obtener información sobre la configuración del resto de los parámetros, consulte **Configuración de Contestadora automática en modo Estándar, página 436**.

Solicitar Administración

En la ficha Solicitar Administración, usted puede:

- Crear saludos utilizando uno de los siguientes métodos:
  - **Grabación de saludos con el grabador de sonidos de CCA**. Este método le permite grabar y reproducir saludos desde dentro de CCA sin usar el grabador de sonidos integrado a CCA. Consulte **Grabar saludos utilizando grabador de sonidos, página 441**.
  - **Carga de saludos grabados previamente desde una PC**. Puede grabar y reproductir archivos .wav en su PC y cargarlos a CUE. El archivo .WAV debe grabarse en formato G.711 u-law, 8-Hz, 8-bit mono (Windows) ó G.711 u-law 44100-Hz mono (Mac)" El saludo no puede durar más que 60 segundos. Consulte **Cargar solicitudes, página 441**.
  - **Use el Sistema de Solicitar Administración de CUE para grabar saludos desde un teléfono**. Para utilizar este método, se configura un anexo para la administración de saludos de AA y se asigna privilegios de administración de saludos a los usuarios. La capacidad de de grabar saludos desde un teléfono elimina la necesidad de una PC o de software de edición de sonidos para administrar los saludos.

    El anexo de administración de saludos es el anexo que marcan los usuarios con privilegios de administración de saludos para grabar o eliminar saludos. Cuando un usuario con privilegios de administración de saludos marca el anexo de administración de saludos, debe indicar su número de anexo y PIN de correo de voz para iniciar sesión. Consulte **Activar la Adminsitración de saludos po teléfono y Asignar privilegios de Solicitar Administración a los usuarios, página 441**.
- Cargar saludos. Consulte **Cargar solicitudes, página 441**.
- Cambio del nombre del archivo de saludos.

  Los nombres de archivos para los saludos creados por usuarios desde teléfnos o por medio de grabador de sonidos incorporado se llaman, inicialmente, User_Prompt_<*time_stame*>.wav.

  Para cambiarle el nombre a un saludo para que se pueda identificarlo fácilmente al asignarle una tecla, haga clic en **Nombre de saludo** en la lista de Saludos disponibles, edite el nombre y luego, haga clic en **Aceptar**.
- Eliminar saludos.

Para eliminar un saludo, haga clic en **Nombre de saludo** en la lista de Saludos disponibles, haga clic en **Eliminar**, y luego, en **Aceptar**.

Grabar saludos utilizando grabador de sonidos

Para grabar saludos para la Contestadora automática o ACD básica con el grabador de sonido integrado, siga estos pasos:

PASO 1 Seleccione la ficha Solicitar Administración en la ventana Contestadora automática.

PASO 2 En la sección **Crear solicitudes, Grabar con grabador de sonido** de la ficha Administración de solicitudes, haga clic en **Abrir**.

PASO 3 Utilice el grabador de sonido integrado para grabar y guardar la solicitud. Consulte **Grabador de sonido, página 442**.

Cargar solicitudes

Para cargar un archivo de solicitud grabado previamente desde su PC:

PASO 1 Seleccione la ficha Solicitar Administración en la ventana Contestadora automática.

PASO 2 En la ventana **Solicitudes disponibles** de la ventana **Administración de solicitudes**, haga clic en **Agregar**.

PASO 3 Haga clic en **Examinar** para ubicar el archivo de la solicitud en su PC.

PASO 4 *Opcional*: Utilice los controles **Reproducir solicitud** para escuchar la solicitud.

PASO 5 Haga clic en **Aceptar**.

Activar la Adminsitración de saludos po teléfono y Asignar privilegios de Solicitar Administración a los usuarios

Para activar la grabación de saludos desde un teléfono en el sistema y asignar privilegios de administración de saludos a los usuarios, siga estos pasos.

PASO 1 Seleccione la ficha Solicitar Administración en la ventana Contestadora automática.

PASO 2 En el campo **Anexo de grabación de saludos**, especifique el anexo para grabar los saludos.

PASO 3 En el campo **Administradores de saludos**, haga clic en **Usuarios**.

PASO 4 En el diálogo **Asignar privilegios de saludos a usuarios**, haga clic en las flechas **Agregar** y **Eliminar** o utilice **Seleccionar todo** para administrar la lista de usuarios seleccionados.

PASO 5 Haga clic en **Aceptar**.

Grabador de sonido

Esta ventana aparece cuando se hace clic en **Grabar** en la ficha Solicitar Administración en la Contestadora automática o en **Grabar** en la ventana Crear/Editar parámetros de ACD básica.

Para grabar saludos para la Contestadora automática o ACD básica con el grabador de sonido integrado, siga estos pasos:

PASO 1 Haga clic en **Grabar** y comience a grabar su mensaje. Se puede pausar, reproducir y detener la grabación.

PASO 2 Cuando quede satisfecho con su grabación, haga clic en **Examinar** para navegar hasta donde desee almacenar el archivo .wav en su PC y especifique un nombre de archivo adecuado para el saludo.

PASO 3 Haga clic en **Aceptar**. Cuando se hace clic en **Aceptar**, CCA cierra el grabador de sonido y guarda el nuevo archivo de saludo en su PC.

Administración del archive de comandos

Se puede cargar, cambiar el nombre y eliminar los comandos personalizados para la Contestadora automática.

Pueden utilizarse hasta tres (3) comandos personalizados definidos por el usuario para AA. Se permite un máximo de
12 comandos; sin embargo, 10 de estas ranuras de comandos están reservadas para los comandos de sistema por defecto para CUE y CCA, los que no pueden eliminarse.

Para comandos personalizados, definidos por el usuario, CCA sólo configura el anexo de AA y en número de PSTN de AA. Debe usar la GUI de CUE para configurar todos los otros parámetros de comandos.

Los comandos para AA que CCA admite (tales como aa_transfer2.aef, aa_sbcs_v02.aef y aa_sbcs_v02.aef) y los comandos para AA por defecto del sistema CUE (tales como aa.aef and aasimple.aef) no pueden eliminarse, modificarse, cambiar de nombre ni sobreescribirse.

Para obtener mayor información sobre cómo crear comandos CUE para AA, consulte la *Guía de escritura y edición de comandos de Unity Express de Cisco*, disponible en Cisco.com.

Procedimientos

Para cargar un comando AA personalizado: siga estos pasos.

PASO 1 En la ficha Administración del archive de comandos de la ventana Contestadora automática, haga clic en **Agregar**.

PASO 2 Haga clic en **Examinar** para ubicar el archivo en su PC.

PASO 3 Haga clic en **Aceptar**.

Para eliminar un archive de comandos AA personalizado, siga estos pasos.

PASO 1 En la ficha Administración del archive de comandos de la ventana Contestadora automática, haga clic en un archive de comandos de la lista disponibles para seleccionarlo.

PASO 2 Haga clic en **Eliminar**.

No se puede eliminar un archive de comandos que la Contestadora automática esté utilizando actualmente.

Distribución básica automática de llamadas (ACD)

Para configurar ACD básica, seleccione **Configurar** > **Telefonía** > **Gestión de llamadas** > **ACD básica** en la barra de funciones.

Esta sección cubre los siguientes temas:

- **Visión general**
- **Antes de comenzar**
- **Crear/Editar parámetros de ACD básica**
- **Configure el servicio ACD básica**
- **Parámetros del informe del grupo de búsqueda**

Visión general

ACD básica (BACD) permite la respuesta y distribución automática de las llamadas entrantes por medio de menús interactivos y grupos de llamado.

Una aplicación ACD básica consiste en un servicio de cola de llamadas y hasta 10 servicios de ACD básica. Para cada servicio ACD básica, se configura un número piloto para el servicvio, parámetros de grupo de búsqueda, saludos, destino para las llamadas no contestadas, tiempo límite de espera, número de reintentos y otros parámetros.

El flujo de llamadas de ACD básica implementado en Configuration Assistant se limita al *modo de desconexión*, en el que la Contestadora automática sirve como el punto de entrada de alto nivel y el control se transfiere a ACD básica para las acciones del menú de segundo nivel.

Cuando se configura una Contestadora automática para el modo de desconexión, ésta envía las llamas entrantes directamente a una cola de llamadas sin entregar opciones de menú a quienes llaman. Una vez en la cola, quien llama escucha un tono si hay un agente disponible o música de espera (MOH) si todos los agentes están ocupados. Si se configura un saludo para el modo de desconexión, quien llama escucha el saludo antes que ésta se envíe a la cola, como se describió. La

caída a través del sistema es simplemente un saludo a los que llaman, se podría decir "Gracias por llamar a XYZ, Inc. Un agente estará con usted en breve." Tome nota que los clientes no puede tomar decisiones interactivas en el modo de desconexión; las llamadas simplemente se contestan y se envían a una cola de llamadas.

Las capacidades de BACD de la plataforma de la serie UC500 se indican a continuación:

- Hata 10 grupos de llamado de BACD (colas de llamadas)
- Hasta 30 llamadas en cada cola
- Hasta 20 agentes pueden ser miembros de un grupo de búsqueda de BACD

CCA versión 2.5 y posteriores agregan la tecla **HLog** en los teléfonos de los agentes BACD. Los agentes ahora pueden iniciar o cerrar sesión en un grupo de búsqueda de BACD usando la tecla **HLog**. La tecla **HLog** se muestra en los teléfonos de agentes cuando se recibe una llamada entrante hacia el grupo de búsqueda de BACD. Los usuarios también pueden acceder a esta tecla desde la pantalla principal del teléfono presionando la tecla **más**. La tecla **HLog** reemplaza el uso de DnD (No molestar) . DnD es menos flexible, ya que deja al suscritpor generalmente no disponible para todas las llamadas, no sólo las llamadas al grupo de búsqueda de BACD.

Consulte **Crear/Editar parámetros de ACD básica, página 447** para ver una explicación de los parámetros de resumen que aparecen en la ventana ACD básica para los servicios BACD configurados.

Antes de comenzar

Antes de configurar ACD básica:

- Defina el flujo de llamadas y las opciones que se presentarán a quien llame.
- Determine cuáles saludos son necesarios y cuáles deberán personalizarse.
- Asegúrese que estén configurados los teléfonos y los usuarios.
- Cuando se configure ACD básica, Configuration Assistant crea automáticamente grupos de llamado para administrar el reenvío de ACD básica. Los parámetros para estos grupos de llamado se configuran en la ventana Crear/Editar parámetros de ACD básica.
- Configure la configuración básica de Contestadora automática. Después que configure el servicio ACD básica, puede seleccionarse la opción

Transferir a ACD básica como acción, que permite que se transfiera el control desde la Contestadora automática al servicio ACD básica.

Configure el servicio ACD básica

Para configurar un servicio de Contestadora automática, siga estos pasos.

PASO 1 En la sección **Resumen de parámetros básicos** de la ventana ACD básica, haga clic en **Crear** o **Modificar**. Se abre la ventana Crear/Editar parámetros de ACD básica.

PASO 2 Configure los parámetros de servicio, los grupos de llamado y los saludos en la ventana Crear/Editar parámetros de ACD básica. Consulte **Crear/Editar parámetros de ACD básica, página 447** para ver información acerca de esta configuración.

PASO 3 Haga clic en **Aceptar** o **Aplicar** y cierre la ventana ACD básica.

Una vez que se ha creado el servicio y su grupo de búsqueda local, la acción **Transferir a ACD básica** ahora está disponible en la ventana Contestadora automática. Seleccione esta acción para que una tecla haga que Contestadora automática transfiera el control al servicio ACD básica cuando quien llame presione la tecla de su teléfono.

Para especificar un servicio ACD básica como la acción para una tecla utilizando la Contestadora automática, siga estos pasos.

Este procedimiento supone que ya se ha configurado los saludos, calendarios y saludos básicos de la Contestadora automática.

PASO 1 Navegue hasta **Configurar** > **Telefonía** > **Gestión de llamadas**>**Contestadora automática**.

PASO 2 Seleccione la ficha Contestadora automática.

PASO 3 Ubique la tecla que quien llame presionará para ser transferido automáticamente al servicio ACD básica que se acaba de configurar y seleccione **Transferir a ACD básica** para el **Modo**.

El campo Parámetros se actualiza automáticamente para mostrar el anexo piloto para el servicio ACD básica. Por ejemplo: **701 (aaService0)**.

Crear/Editar parámetros de ACD básica

La ventana Crear/Editar parámetros de ACD básica aparece cuando se hace clic en **Crear** o **Modificar** en la ventana ACD básica (**Configurar** > **Telefonía** > **Gestión de llamadas**>**ACD básica**).

Parámetros de servicio

Configure los parámetros de servicio como se describe a continuación para cada servicio ACD básica. Pueden configurarse hasta 10 servicios ACD básica.

Configuración	Descripción
Número piloto	Anexo para este servicio ACD básica. Este es el número que disca la Contestadora automática cuando se ejecuta la acción Transferir a ACD básica.
Desvío sin respuesta	Destino para las llamadas no contestadas por el grupo de búsqueda de B-ACD, ya sea porque todos los agentes han cerrado sesión o están ocupados, o porque se ha superado el límite máximo de reintentos de llamada. Las llamadas no contestadas pueden reenviarse a la Contestadora automática, al Grupo de búsqueda o al de envío, al Correo de voz, a un anexo interno o a Otro número (número PSTN externo).
Reproducir tono de ocupado en x segundos	Es la cantidad de segundos que se espera antes de reproducir el tono de ocupado de ACD básica. Se trata del mismo retardo entre cuando quien llama se une a la cola de B-ACD y cuando se reproduce el segundo saludo por primera o segunda vez. Se utiliza el mismo intervalo de tiempo entre las repeticiones del segundo saludo. Los valores válidos varían entre 30 y 120 segundos. El valor por defecto es 60 segundos. El archivo del tono de ocupado por defecto es en_bacd_allagentsbusy.au.
Sin repuesta enviar a en x segundos	Lapso máximo para reintentos de llamadas antes que ésta se reenvíe al destino especificado en **Sin respuesta enviar a**. Es la cantidad máxima de tiempo que una llamada puede estar en la cola de llamadas. Los valores válidos varían entre 60 y 3600 segundos. El valor por defecto es 600 segundos.

Configuración	Descripción
Reintentar con número en x segundos	Cantidad de segundos que se espera antes de volver a enviar la llamada al grupo de búsqueda local para este servicio B-ACD.
Tranferencia a solicitud BACD	*Opcional*. Este es el nombre de archivo de la solicitud para Transferir a B-ACD.
Saludo de bienvenida	*Opcional*. Este es el nombre de archivo del saludo de bienvenida de B-ACD.
Máximo de reintentos antes de desconectar la llamada	Número de veces de reintentos con el destino especificado para **Sin respuesta reenvío a** antes de rechazar la llamada. Cuando se rechaza la llamada, se reproduce el tono de desconexión de ACD básica. Los valores válidos varían entre 1 y 3. El valor por defecto es 1.

Parámetros del Grupo de búsqueda

Configure los parámetros del grupo de búsqueda como se describe a continuación para cada servicio ACD básica. El grupo de búsqueda de ACD básica que se crea es local al servicio ACD básica.

Configuración	Descripción
Tipo de búsqueda	Define el orden en el que se distribuyen las llamadas a los miembros del grupo de búsqueda de ACD básica. Seleccione uno de los siguientes tipos: ▪ **secuencial**. Las llamadas se envian a los miembros del grupo de búsqueda de ACD básica en el orden en que aparecen en el diálogo Miembros. ▪ **par**. Las llamadas se envían a los miembros del grupo de búsqueda de ACD básica en un orden al azar. ▪ **desocupado más tiempo**. Las llamadas se envían al miembro del grupo de búsqueda de ACD básica con el tiempo desocupado más largo.
Miembros	Haga clic en **Miembros** para abrir un diálogo para seleccionar teléfonos y sus usuarios asociados como miembros de este grupo de búsqueda de ACD básica. Consulte **Miembros del grupo de búsqueda, página 450**.

Configuración	Descripción
Límite de tiempo de búsqueda	Número de segundos antes que una llamada no contestada por un número del grupo de búsqueda sea dirigida al siguiente miembro, según lo especifica el Tipo de búsqueda. Por defecto, son 8 segundos.
Activar Cierre de sesión automático	Cuando se marca esta opción, se activa el cierre de sesión automático. Cuando se supera el valor de **Intentos antes de cerrar sesión**, el teléfono del agente queda automáticamente con su sesión cerrada en el grupo de búsqueda de ACD básica.
Todos los agentes con sesión cerrada muestran el mensaje	Mensaje que se mostrará cuando todos los agentes (miembros del grupo de búsqueda) tengan cerrada su sesión. Por defecto, todos los agentes tienen su sesión cerrada. El mensaje puede tener hasta 39 caracteres.
Intentos antes de cerrar la sesión	Cantidad máxima de llamadas no contestadas hacia el miembro del grupo de búsqueda B-ACD (de 1 a 20) antes de cerrar la sesión automática. El valor por defecto es 3.

Solicitudes

Para administrar las solicitudes de ACD básica, realice la configuración como se describe a continuación. Cuando haya finalizado de hacer cambios, haga clic en **Aceptar** o **Aplicar**.

Configuración	Descripción
Saludo de bienvenida	Seleccione una de las solicitudes por defecto para ACD básica o haga clic en **Grabar** para grabar una solicitud personalizada utilizando el grabador de sonido incorporado.
Transferir al saludo de B-ACD básica	Seleccione una de las solicitudes por defecto para ACD básica o haga clic en **Grabar** para grabar una solicitud personalizada utilizando el grabador de sonido incorporado.

Miembros del grupo de búsqueda

Esta ventana aparece cuando se hace clic en el botón **Miembros** de la ventana Crear/Editar parámetros de ACD básica.

Para crear o editar la lista de miembros del grupo de búsqueda y sus teléfonos asociados, siga estos pasos.

PASO 1 Haga clic en un usuario de la lista Disponible o Seleccionado. Utilice los accesos directos del teclado CTRL-clic o SHIFT-clic para seleccionar múltiples usuarios en cualquiera de las listas.

PASO 2 Utilice los botones **Agregar**, **Eliminar** y **Seleccionar** todo para mover a los usuarios seleccionados entre las listas Disponible y Seleccionado.

PASO 3 Utilice las feclas **Hacia arriba** y **Hacia abajo** para ordenar a los miembros del grupo de búsqueda.

PASO 4 Haga clic en **Aplicar** para aplicar los cambios.

Parámetros del informe del grupo de búsqueda

La función ACD básica utiliza el generador de informes CME de B-ACD para crear archivos simples de informes en formato CSV que pueden importarse en un programa de planilla de cálculo.

Para activar los informes de ACD básica y configuirar los parámetros de los informes del grupo de búsqueda, complete los campos en la sección Parámetros del informe del grupo de búsqueda de la ventana, como se decribe a continuación.

Cuando haya finalizado de configurar los parámetros del informe del grupo de búsqueda de ACD básica, haga clic en **Aceptar** o en **Aplicar**.

Configuración	Descripción
Activar informe CME	Cuando está marcado, se activa la generación del informe del grupo de búsqueda de ACD básica. Por defecto, está activado el informe de ACD básica.

Configuración	Descripción
Ubicación del informe CME	Ubicación del servidor TFTP o FTP y del directorio para los informes de ACD básica. El formato es **tftp://** *<Dirección IP del servidor>/<directorio>/<nombre>* o **ftp:***//<Dirección IP del servidor>/<directorio>/<nombre>*. Por ejemplo: **tftp://192.168.10.1/bacdrpts/mybacd**
Número de informes	El número de archivos de informes con formato CSV simple que va a crearse. Los valores válidos son del 1 al 200.
Frecuencia de informes (hrs)	Frecuencia de la generación de informes, en horas. Los valores válidos son del 1 al 84.
Carga manual de informes	Si se activan los informes CME, haga clic en *Carga manual de informes* para activar de inmediato el envío de los datos del informe a una uicación de informe específica en el servidor TFTP. Esta opción no está disponible cuando está desactivado el informe CME.

Atención nocturna

Para configurar los Atención nocturna, seleccione **Configurar** > **Telefonía** > **Gestión de llamdas**> **Atención Nocturna** en la barra de funciones.

Antes de poder activar los Atención nocturna, se debe configurar un atención nocturna en la ficha Programa de atención nocturna de la ventana Calendarios (**Configurar** > **Telefonía** > **Gestión de llamadas**> **Calendarios**). Consulte **Atención nocturna, página 433**.

Visión general

Pueden configurarse hasta cuatro anexos para los atención nocturna. Cada anexo puede configurarse con un número de Desvío de llamadas o con una Campanilla de atención nocturna.

Cuando se configura un número de desvío de llamadas para un anexo de atención nocturna, las llamadas entrantes a dicho anexo durante las horas de atención nocturna se desvían a dicho anexo.

La campanilla de atención nocturna permite entregar cobertura para anexos sin personal durante las horas de atención nocturna. During night-service hours, extensions configured for night-service bell receive notification of incoming calls with a special “burst” ring. Los usuarios telefónicos en los teléfonos de atención nocturna pueden utilizar la función de contestación de llamadas para responder a las llamadas entrantes.

Para configurar los teléfonos de servicios nocturno, al menos uno de los anexos debe configurarse con una campanilla de atención nocturna.

Un usuario puede especificar un código de atención nocturna para manualmente apagar y encender el tratamiento de atención nocturna desde cualquier teléfono que tenga un anexo asignado para atención nocturna. El código para pasar a servicio ncturno activa o desactiva este servicio para todos los teléfonos con atención nocturna.

Se aplican las siguientes limitaciones al atención nocturna:

- Los teléfono analógicos no reciben notificaciones de atención nocturna. Sin embargo, los anexos para los teléfonos analógicos que se configuran con un perfil de Teléfono de usuario pueden configurarse para que se monitoreen durante el atención nocturna.
- Los teléfonos IP que no tienen teclas pueden usar códigos de acceso de funciones para contestar llamadas hacia el anexo de atención nocturna.

Procedimientos

Para configurar un anexo de atención nocturna con un número de desvío de llamadas:

PASO 1 En el campo **Anexo #**, seleccione un anexo disponible de la lista desplegable.

PASO 2 En el campo **Tipo de respuesta**, seleccione **desvío de llamadas atención nocturna**.

PASO 3 Especifique un número de grupo en el campo **Desviar a número**.

Las llamadas entrantes a este anexo durante las horas de atención nocturna se desvían hacia este número.

Este número puede ser un número PSTN externo o un anexo. Cuando se especifica un número PSTN externo, especifique el número exactamente como lo marcaría, incluyendo el código de acceso.

PASO 4 Repita los pasos 1 al 3 para configurar el atención nocturna con un número de desvío de llamadas para más anexos.

PASO 5 Haga clic en **Aceptar** o **Aplicar**.

Para configurar el Atención nocturna con campanilla de atención nocturna, siga estos pasos:

PASO 1 En el campo **Anexo #**, seleccione un anexo disponible de la lista desplegable.

PASO 2 En el campo **Tipo de respuesta**, seleccione **campanilla de atención nocturna**.

PASO 3 Haga clic en el botón **Teléfonos de atención nocturna** para abrir una ventana para seleccionar los teléfonos.

PASO 4 Seleccione los teléfonos de la lista de teléfonos disponibles.

PASO 5 Haga clic en **Agregar**.

PASO 6 Haga clic en **Aceptar** o **Aplicar**.

Para configurar un código de atención nocturna, siga estos pasos.

PASO 1 En el campo **Código de atención nocturna**, especifique el código para activar el atención nocturna.

Es posible especificar hasta 15 dígitos. CCA automátically asigna un prefijo al código con un asterisco (*).

Al seleccionar un código para pasar a Atención nocturna, tenga presente que CCA envía un conjunto de códigos de activación de funciones por defecto (usado principalmente para líneas analógicas) al UC500. Para evitar el traslape con estos códigos de activación de funciones, el código para pasar a Atención nocturna debe comenzar con *2, *7, *8, ó *9.

PASO 2 Haga clic en **Aceptar** o **Aplicar**.

paraquitar un anexo de atención nocturna, configure el campo **Anexo #** como **Ninguno** y aplique el cambio. También puede seleccionar un anexo diferente y modificar cualquiera de los demás valores.

Para modificar la lista de teléfonos de atención nocturna, haga clic en **Teléfonos de atención nocturna**, utilice los botones **Agregar**, **Quitar**, y **Seleccionar todos** para actualizar la lista de Teléfonos seleccionados y aplique los cambios.

Para obtener más información, consulte estos temas:

- **Teléfonos de Atención nocturna, página 454**
- **Atención nocturna, página 433**

Teléfonos de Atención nocturna

Esta ventana aparece cuando se hace clic en **Teléfonos de atención nocturna** en la ventana Atención nocturna.

Haga clic en los teléfonos de la lista **Disponibles** y utilice los botones de flecha **Agregar**, **Quitar**, y **Seleccionar todo** para desplazar los teléfonos entre las listas de Teléfonos Disponibles y Seleccionados.

Los teléfonos seleccionados se configuran como teléfonos de atención nocturna y recibirán una notificación de llamadas entrantes cuando esté activo el atención nocturna. Los usuarios telefónicos en los teléfonos de atención nocturna pueden presionar el botón **GPickUp** en su teléfono para responder a las llamadas entrantes.

Cuando termine de seleccionar teléfonos, haga clic en **Aceptar**.

Para obtener más información, consulte estos temas:

- **Atención nocturna, página 451**
- **Atención nocturna, página 433**

Grabación en vivo

Esta ventana aparece cuando se selecciona **Configurar** > **Telefonía** > **Gestión de llamadas> Grabación en vivo**en la barra de funciones.

Visión general

Grabación en vivo permite que los usuarios graben conversaciones y almacenen la grabación como mensaje en su buzones de entrada. Luego, se pueden reproducir o enviarlo a otro buzón de correo de voz. La configuración por defecto para esta aplicación es desactivada.

Los usuarios telefónicos pueden iniciar una sesión de Grabación en vivo presionando la tecla **LiveRcs** de su teléfono IP durante una llamada. El sistema establece una conferencia telefónica entre el número piloto de Grabación en vivo que se configura aquí y la contraparte que se grabará.

Se reproducen tonos periódicamente para indicar que la llamada se está grabando. Se puede seleccionar si estos tonos están activados o desactivados y configurar su duración e intervalos.

Las siguientes notas se aplican a la grabación en vivo:

- Quien llame desde el exterior no puede usar esta función porque usa el número del anexo asignado a quien llama.
- Los mensajes de la grabación en vivo no activan un mensaje de notificación cuando se envían a un buzón de correo de voz.
- El tamaño de los mensajes de Grabación en vivo sólo está limitado por la cantidad de espacio restante en el buzón de voz del suscriptor.

Procedimientos

Para activar y configurar Grabación en vivo, siga estos pasos.

PASO 1 Configuración de la **grabación en vivo**:

a. Marque la opción **Activar grabación en vivo** para activar esta función.

b. En el campo Número piloto, indique el número del anexo piloto de la función Grabación en vivo.

   Este anexo se usa para enviar todas las llamadas entrantes a este número piloto del sistema de correo de voz. Todas las llamadas enviadas al número piloto del correo de voz desde este número omitirán el saludo del correo de voz. Si quien llama tiene un buzón de correo de voz, la grabación comenzará de inmediato.

PASO 2 Configuración del **Tono de grabación en vivo**:

a. La configuración de **Duración del bip** especifica el número de milisegundos que se reproducirá el tono. La duración del bip puede variar entre 50 y 1000 milisegundos. El valor por defecto es 250 milisegundos.

b. El **Intervalo del bip** especifica el número de milisegundos entre el término de un bip y el inicio del siguiente. El intervalo de del bip puede variar entre 1 y 30 segundos. El intervalo del bip por defecto es de 15 segundos.

PASO 3 Haga clic en **Aceptar** o **Aplicar**.

T.37 Facsímil a correo

Para configurar T.37 Facsímil a corre, seleccione **Configurar** > **Telefonía** > **Gestión de llamadas**> **T.37 Facsímil a correo** en la barra de funciones.

Para averiguar más sobre las funciones T.37 Facsímil a correo electrónico y su configuración, consulte los siguientes temas:

- **Visión general**
- **Limitaciones**
- **Prerequisitos para configurar T.37 Facsímil**
- **Activación de T.37 Facsímil a correo y configuración de servicios**
- **Configuración de buzones de correo para los facsímiles entrantes**

Visión general

T.37 es un estándar ITU para enviar mensajes de facsímil por medio del correo electrónico. La función T.37 Facsímil a correo de CCA permite que el UC500 actúe como un portal de facsímil para comunicarse con máquinas de facsímil normales, convertir facsímiles en correos electrónicos o viceversa. En Cisco, esta función también se conoce como T.37 Guardar y enviar facsímil.

La función T.37 Facsímil a correo de CCA permite configurar el UC500 y el sistema de correo de voz para que provean las siguientes funciones:

- **Servicios de facsímil entrante**, usando la aplicación En Rampa.

  Usando CCA, se configuran los buzones de correo de voz que recibirán los facsímiles entrantes. Los facsímiles guardados pueden enviarse como adjuntos de correos electrónicos o enviarse a una impresora. Los mensajes de facsímil se convierten en archivos de imagen con formato TIFF. Se puede configurar los buzones de correo para servicio de sólo facsímil (todas las llamadas entrantes se suponen como llamadas de facsímil) o para servicio de voz y de facsímil (las llamadas entrantes pueden ser de voz o de facsímil).

  CCA configura buzones de correo de voz para usuarios, grupos y anexos flotantes (anexos no asociados a un teléfono o grupo). Todos los buzones de correo, incluyendo los asociados a anexos flotantes, pueden recibir y guardar correo con facsímil, siempre que estén asociados a un número de teléfono entrante en un enlace PSTN.

- **Detección de voz y facsímil**, usando la aplicación Detección de voz y facsímil.

  La detección de voz y facsímil entrega la capacidad de detectar si una llamada entrante es voz o facsímil. Esto permite que se use un solo número entrante tanto para las llamadas de voz como para las de facsímil.

- **Impresión de facsímil**, usando la aplicación Fuera de rampa. Esto permite que los usuarios telefónicos usen la Interfaz de usuario telefónico (TUI) para enviar facsímiles guardados en el correo de voz a una máquina de facsímil local para su impresión.

- **Recibir facsímiles como mensajes de correo electrónico**. Usando CCA, se puede integrar los servicios de T.37 Facsímil a correo con los servicios de notificación de correo de voz o IMAP para que los usuarios puedan recibir notificación de los facsímiles entrantes por medio del teléfono o del correo electrónico, con la opción de incluir al facsímil como archivo adjunto del correo electrónico.

- **Grabe solicitudes personalizadas o use las solicitudes por defecto del sistema para las llamadas entrantes hacia líneas configuradas para recibir tanto llamadas de voz como de facsímiles**. Puede usar las solicitudes por defecto para las llamadas entrantes hacia línea con detección de voz y facsímil o se pueden configurar solicitudes personalizadas. Las solicitudes por defecto se entregan en Inglés, Español y Chino.

CCA agrupa las aplicaciones de Respuesta de voz interactiva (IVR) usadas para los servicios de facsímil, detección de facsímil e impresión de facsímil. Estas aplicaciones se implementan como comandos de "Idioma de comandos total (TCL) y se cargan en la memoria flash del UC500 cuando se aplica la configuración T.37 Facsímil a correo. Los comandos por defecto presentados a los usuarios para las llamadas entrantes a las líneas configuradas con detección de voz y facsímil se cargan en la memoria flash cuando se aplica la configuración.

Los comandos TCL de la aplicación y las solicitudes del sistema por defecto se ubican en el directorio `flash:applications/faxmail` de la memoria flash del UC500. Sus solicitudes personalizadas se ubican en el directorio `flash:applications/faxmail/custom` de la memoria flash.

Limitaciones

Se aplican las siguientes limitaciones a la configuración T.37 Facsímil a correo usando CCA:

- Sólo los buzones de correo asociados a números de teléfonos entrantes en enlaces PSTN pueden configurarse para recibir facsímiles entrantes. No se admiten enlaces SIP.
- La función Detección de voz y facsímil no funciona con todas las máquinas de facsímil ni con todos los modos de operación. Puede no detectarse tonos correctamente para las máquinas de facsímil que operen en modo manual.
- No se admite el uso simultáneo de la aplicación T.37 Detección de facsímil y SNR.
- Los teléfonos que no tienen una Interfaz de usuario telefónico (TUI) no pueden usarse para enviar facsímiles a una máquina de facsímil local para su impresión.

Prerequisitos para configurar T.37 Facsímil

Antes de activar y configurar T.37 Facsímil, debe establecerse la siguiente configuración:

- Configuración de usuarios, anexos y buzones de correo de voz en el sistema.

  Para hacerlo, vaya a **Configurar** > **Telefonía** > **Usuarios y anexos** > **Usuarios y teléfonos** y seleccione la ficha Anexos de usuarios o Anexos flotantes. Se debe tener presente que los buzones de correo de voz para los grupos de llamado y los grupos de envío de llamadas se crean cuando la opción Desvío sin respuesta se configura como Correo de voz en la ventana Grupos de teléfonos (**Configurar** > **Telefonía** > **Grupos de teléfonos**).
- Sólo los buzones de correo de voz asociados a números de teléfonos entrantes en enlaces PSTN pueden configurarse para recibir facsímiles entrantes. Se debe crear un plan de numeración entrante para cada anexo con un buzón de correo de voz que se configurará para recibir los facsímiles entrantes.

  Para hacerlo, vaya a **Configurar** > **Telefonía** > **Plan de numeración** > **Entrante**. Al seleccionar un Tipo de destino para las llamadas FXO entrantes o Discado directo a la contestadora automática, grupos u operador, seleccione OPERATOR o HUNT_GROUP como el tipo de destino.
- Si desea activar la función Impresión de facsímil se debe tener una máquina de facsímil local conectada a un puerto FXS del UC500 y el puerto FXS

debe tener asignado el perfil de FAX. Para hacerlo, vaya a **Configurar** > **Telefonía** > **Puertos y enaleces** > **Puertos FXS**.

- Para integrar a T.37 Facsímil a correo con las notificaciones de correo de voz para que los usuarios puedan recibir la notificación por correo electrónico de los facsímiles entrantes con el facsímil como archivo adjunto, vaya a **Configurar** > **Telefonía** > **Usuarios y teléfonos** > **Correo de voz** y configure las notificaciones para los buzones de correo que se configurarán como los receptores de los facsímiles entrantes.

  Para ver instrucciones sobre cómo hacerlo, consulte **Notificaciónes, página 387**.

  NOTA: Para recibir notificaciones por teléfono o por correo electrónico de facsímiles entrantes, el Nivel de configuración debe estar configurado como Todo correo de voz.

- También se puede activar la función Mensajería unificada en CCA para integrar T.37 Facsímil a correo con IMAP. Para activar la función Mensajería unificada, vaya a **Aplicaciones** > **Smart Applications** >**Administrador de Smart Applications**. Consulte **Mensajería unificada (IMAP), página 529**.

Activación de T.37 Facsímil a correo y configuración de servicios

En la ficha Servicios, se puede:

- Activar los servicios de T.37 Facsímil a correo
- Configurar las solicitudes para la Detección de voz y facsímil
- Configurar la impresora de facsímiles por defecto para la Impresión de facsímiles

Para activar y configurar T.37 Facsímil a correo, siga estos pasos.

PASO 1 En el menú desplegable Nombre del host del dispositivo, seleccione UC500.

PASO 2 Haga clic en la casilla **Activar T.37 Facsímil a correo**.

PASO 3 Complete los campos de la ficha Servicios como se muestra en la siguiente tabla.

Configuración	Descripción
Sólo facsímil entrante	La sección Sólo facsímil entrante de esta página muestra la versión de la aplicación Sólo facsímil en rampa que está instalada. Si T.37 fax a correo no se ha configurado para el sistema, el mensaje "A la espera de instalación (versión 2.0.1.3)" aparece. La aplicación En rampa se cargará e instalará en el UC500 cuando se aplique la configuración.
Voz y Facsímil entrante	La detección de voz y facsímil entrega la capacidad de detectar si una llamada entrante es voz o facsímil. Esto permite que se use un solo número entrante tanto para las llamadas de voz como para las de facsímil. CCA configura la detección de fax para "escuchar primero" para que la llamada no necesita estar conectado. Cuando se detecta un todo de facsímil en la llamada, se procesa y rutea como una llamada de facsímil. Si no se detecta tono de facsímil, se rutea como una llamada de voz normal. La versión de la aplicación Detección de voz y facsímil que está instalada también se muestra acá. Si T.37 fax a correo no se ha configurado para el sistema, el mensaje "En espera de instalar" y la versión de la Voz y la aplicación de detección de fax se muestran. La aplicación Detección de voz y facsímil se cargará e instalará en el UC500 cuando se aplique la configuración.

Configuración	Descripción
Voz y Facsímil entrante (continuación)	**Solicitud para llamadas entrantes** El proceso de detección puede retrasar las llamadas entrantes hasta 9 segundos. Las solicitudes de sistema por defecto se entregan para alertar a quien llama y dar opciones para que quienes llamen eviten el retraso y se conecten de inmediato o envíen un facsímil. También se puede grabar una solicitud personalizada para estos fines (por ejemplo, es posible que desee hacerlo si necesita que la solicitud se reproduzca en un idioma diferente). El valor por defecto del sistema es “Para enviar un fax, pulse la tecla START en su máquina de fax ahora. Para llamadas de voz, pulse cualquier tecla o permanecer en la línea.” Seleccione una de las siguientes opciones: ▪ **Personalizada**. Graba una solicitud personalizada para las llamadas entrantes. Cuando se seleccione, haga clic en **Agregar archivo** para guardar y cargar una solicitud personalizada. ▪ **Sistema (Chino)**. Usa el idioma chino para las solicitudes del sistema por defecto. ▪ **Sistema (Inglés)**. Usa el idioma inglés para las solicitudes del sistema por defecto. Éste es el valor predeterminado. ▪ **Sistema (Español)**. Usa el idioma español para las solicitudes del sistema por defecto. ▪ **Ninguno** Seleccione esta opción si no está usando la función Detección de voz y facsímil (los buzones de correo que reciben facsímiles entrantes se configuran como Sólo facsímil). El servidor TFTP incorporado en CCA se usa para cargar y descargar las solicitudes del sistema. Asegúrese que la configuración de firewall de su PC permita el tráfico TFTP desde y hacia el UC500 y que no hay servidores TFTP de terceros ejecutándose en su PC. Para ver instrucciones sobre cómo grabar solicitudes usando el grabador de solicitudes de CCA, consulte **Grabador de sonido, página 442**.
	Archivo de solicitud personalizada (Opcional) Muestra el nombre del archivo de la solicitud que se grabó para las llamadas entrantes. Este menú sólo aparece si se graba una solicitud personalizada.

Configuración	Descripción
Impresión de facsímil	El correo de fax puede imprimirse en cualquier número discable o en la impresora de fax configurada por defecto. Si desea activar la función Impresión de facsímil se debe tener una máquina de facsímil local conectada a un puerto FXS del UC500 y el puerto FXS debe tener asignado el perfil de FAX. Para hacerlo, vaya a **Configurar** > **Telefonía** > **Puertos y enaleces** > **Puertos FXS**. Sólo los puertos FXS a los que se les ha asignado un perfil de Facsímil están disponibles para selección. La versión de la aplicación Impresión de facsímil fuera de rampa que está instalada también se muestra acá. Si T.37 fax a correo no se ha configurado para el sistema, el mensaje "A la espera de instalación (versión 2.0.1.1)" aparece. La aplicación Impresión de facsímil en rampa se cargará e instalará en el UC500 cuando se aplique la configuración.
	Impresora de facsímil por defecto Para configurar una impresora de facsímil por defecto: 1. Seleccione la impresora por defecto que se usará. 2. Haga clic en **Aceptar** o **Aplicar**.

Configuración de buzones de correo para los facsímiles entrantes

Los facsímiles entrantes pueden guardarse y enviarse a buzones de correo de voz. Todos los buzones de correo pueden recibir facsímiles, siempre y cuando tengan un plan de numeración entrante. El mismo buzón de correo se usa para guardar facsímiles y correos de voz.

Además, se puede desactivar el facsímil sin impactar los mensajes existentes en el buzón de correo. Sin embargo, una vez que se desactiva la función de facsímil para un buzón de correo, el sistema rechaza facsímiles dirigidos a ese buzón de correo desde una máquina de facsímiles.

Los buzones de correo configurados con un destino de correo electrónico pueden recibir facsímiles como correo electrónico. Para configurar los destinos de correo electrónico, vaya a **Telefonía** > **Usuario y anexos** > **Correo de voz** y seleccione la ficha Notificaciones para activar la notificación por correo electrónico.

NOTA: La función Mensajería unificada también puede usarse para recibir facsímiles como correo electrónico. Para configurar la función Mensajería unificada, vaya a **Aplicaciones** > **Smart Applications** > **Administrador de Smart Applications**.

Agregar buzones de correo para recibir los facsímiles entrantes

Sólo pueden agregarse los buzones de correo asociados a los números entrantes en los enlaces PSTN. Para configurar los números entrantes, vaya a **Telefonía** > **Plan de numeración** > **Entrante**.

Para agregar buzones de correo que recibirán facsímiles entrantes, siga estos pasos:

PASO 1 Haga clic en **Agregar** en la ficha Buzones de correo de la ventana T.37 Facsímil a correo electrónico. Aparecerá la ventana Agregar buzones de correo para recibir facsímiles entrantes.

PASO 2 En la ventana Agregar buzones de correo para recibir facsímiles entrantes, use los botones **Agregar**, **Eliminar**, y **Seleccionar todos** para desplazar a los usuarios seleccionados entre las listas Buzones de correo disposnibles y Buzones de correo seleccionados.

PASO 3 Haga clic en **Aceptar** para volver a la ventana de T.37 Facsímil a correo electrónico.

Elilminación de buzones de correo de la lista

Para eliminar buzones de correo que recibirán facsímiles entrantes, siga estos pasos:

PASO 1 En la ficha Buzones de correo, seleccione el buzón de correo deseado

PASO 2 Haga clic en **Eliminar**.

PASO 3 Haga clic en **Aceptar** o **Aplicar**.

15

Plan de numeración

Esta sección cubre la configuración del plan de numeración entrante y saliente, incluyendo los siguientes temas:

- **Plan de numeración entrante**
- **Plan de numeración saliente**
- **Grupos de enlaces PSTN**
- **Plantillas de plan de numeración**

Plan de numeración entrante

Para configurar el plan de numeración entrante, seleccione **Configurar** > **Telefonía** > **Plan de numeración** > **Entrante** de la barra de herramientas.

Antes de comenzar

Antes de configurar el plan de numeración para el discado directo y para llamadas FXO entrantes, asegúrese que se haya configurado la configuración de la ventana Enlaces PSTN para los enlaces BRI, PRI y FXO (**Configurar** > **Telefonía** > **Puertos y enlaces**> **Enlaces PSTN**). Si se utilizan enlaces SIP, asegúrese que estos están configurados (**Configurar** > **Telefonía** > **Enlaces** > **Enlaces SIP**). Contestadora automática, grupos de llamado y grupos de envío de llamadas también deberían configurarse para que estén disponibles como destinos para las llamadas FXO entrantes y los números DID.

La ventana del plan de numeración entrante tiene las siguientes fichas:

- **Llamadas FXO entrantes**
- **Discado directo**

Llamadas FXO entrantes

En la ficha Llamadas FXO entrantes, seleccione el destino para las llamadas entrantes en los puertos FXO.

Para configurar los destinos para las llamadas entrantes a puertos FXO, seleccione un puerto FXO de la lista, edite la configuración como se describe a continuación y, luego, haga clic en **Aceptar** o **Aplicar**.

Campo	Descripción
Descripción	Descripción de este puerto FXO. Se puede editar el valor por defecto, que inicialmente es el mismo que el número del puerto FXO, por ejemplo, 4 FXO-0/0/1.
Enlace	Campo de sólo lectura que contiene el número del puerto FXO, por ejemplo, 4 FXO-0/0/1.
Tipo de Destino	Destino para las llamadas entrantes a este enlace FXO. Seleccione de entre los siguientes tipos de destino. ▪ CO_LINE (direct “Central Office” PSTN trunk line) ▪ OPERATOR (OPERADORA) ▪ CONTESTADORA_AUTOMÁTICA ▪ GRUPO_DE_ENVÍO ▪ GRUPO_DE_BÚSQUEDA ▪ B_ACD (Anexo de servicios ACD básico)
Destino	Si selecciona CONTESTADORA_AUTOMÁTICA, GRUPO_DE_BÚSQUEDA,GRUPO_DE_ENVÍO ó B_ACD como tipo de anexo, seleccione el anexo o grupo adecuado de la lista que está configurada en su sistema. Si selecciona Operadora como el tipo de anexo, especifique manualmente el anexo que se va a utilizar para la Operadora del sitio. Si selecciona CO_LINE, se muestra una descripción de sólo lectura, por ejemplo, Línea de enlace directo - CO1.

Discado directo

En la ficha Discado directo, defina normas de traducción para el mapeo de los números PSTN entrantes hacia anexos internos. Pueden definirse dos tipos de traducciones:

- **Discado directo a anexos de usuario interno.** Configure los números de discado directo entrante (DID) para que campanilleen en anexos internos. Utilice este método para crear un mapeo uno a uno entre un solo número DID y un solo anexo interno. Consulte **Discado directo a anexos de usuario interno, página 469**.
- **Discado directo a AA, Grupos, Operadora.** Configure un número DID o intervalo de números DID para que campanilleen en un anexo de grupo de búsqueda, grupo de envío de llamadas, servicio ACD básica, Contestadora automática o de Operadora. Consulte **Discado directo a Contestadora automática, Grupos, Operadora, página 471**.

IMPORTANTE Para enlaces SIP, el mapeo DID para la Contestadora automática y anexos de correo de voz deben configurarse por medio de la configuración de las ventanas de Contestadora automática y de Correo de voz, no a través de la configuración DID de la ventana Plan de numeración entrante.

Discado directo a anexos de usuario interno

Esta ventana aparece cuando se hace clic en **Agregar** en la sección Discado directo a anexos de usuario interno en la ventana Plan de numeración entrante.

Visión general

En esta ventana, se configuran números DID (discado directo entrante) para que campanilleen en anexos de usuarios internos. Ello se realiza creando normas de traducción para definir el mapeo entre cada número DID y su anexo interno correspondiente. Un solo número DID se mapea hacia un solo anexo interno.

El número DID que su portador le entregue puede tener cualquier cantidad de dígitos. Consulte con su portador acerca de los DID que se han asignado a su instalación.

El número máximo de normas de traducción DID es 15. Sin embargo, una sola norma de traducción puede utilizarse para mapear múltiples números DID hacia anexos internos utilizando un intervalo, según se muestra en este ejemplo.

Configuración de traducción DID	
Configuración	**Valor**
Inicio del intervalo DID	9725551000
Término de intervalo DID	9725551005
Inicio de número interno	200
Término de número interno	205
Configuración resultante	
Llamadas entrantes a este número DID	**Llamar a este anexo**
972-555-1000	Anexo 200
972-555-1001	Anexo 201
972-555-1002	Anexo 202
972-555-1003	Anexo 203
972-555-1004	Anexo 204

Procedimientos

Para configurar una norma de traducción para el discado directo hacia anexos de usuarios internos, haga clic en **Agregar**, complete los campos de la ventana Discado directo hacia anexos de usuarios internos como se describe a continuación y haga clic en **Aceptar** o **Aplicar**.

Campo	Descripción
Descripción	Descripción del mapeo de anexos DID.
Enlaces	Seleccione el tipo de enlace digital de la lista que corresponda al portador que entrega los números DID, por ejemplo, Enlace SIP, Enlace BRI o Enlace PRI.

Campo	Descripción
Números DID	Números DID (PSTN) que mapean hacia los anexos internos correspondientes. ▪ Para mapear sólo un número, especifique el mismo número para el **Inicio del intervalo DID** y **Término del intervalo DID**. ▪ Para mapear un intervalo de números, especifique los números iniciales y finales que definen el intervalo. ▪ DID numbers can begin with a “+” character.
Números internos	Números de anexos internos que mapean hacia los números DID. ▪ Para mapear sólo un número, especifique el mismo número para el **Inicio del número interno** y **Término del número interno**. ▪ Para mapear un intervalo de números, especifique los números iniciales y finales de anexos internos que definen el intervalo. ▪ La cantidad de anexos internos especificados en el intervalo debe coincidir con la cantidad de números DID que especifica el intervalo DID.

Discado directo a Contestadora automática, Grupos, Operadora

Esta ventana aparece cuando se hace clic en **Agregar** en la sección Discado directo a contestadora automática, Grupos, Operadora en la ventana Plan de numeración entrante.

En esta ventana se crean las traducciones DID que mapean uno o más números PSTN entrantes hacia una Contestadora automática, grupo de búsqueda, grupo de envío de llamadas, servicio ACD básica u operadora.

Para configurar el discado directo desde uno o más números PSTN hacia un grupo de búsqueda, grupo de envío, servicio ACD básico, anexo de operadora o hacia la Contestadora automática, haga clic en **Agregar**, complete los campos de la ventana **Discado directo a Contestadora automática, Grupos, Operadora** como se describe a continuación y, luego, haga clic en **Aceptar** o **Aplicar**.

Campo	Descripción
Descripción	Descripción del mapeo de anexos DID.
Enlaces	Seleccione el tipo de enlace de voz de la lista que corresponda al portador que entrega los números DID, por ejemplo, Enlace SIP, Enlace BRI o Enlace PRI.
Números DID	Números DID (PSTN) que mapean hacia los destinos internos correspondientes. ▪ Para mapear sólo un número, especifique el mismo número para el **Inicio del intervalo DID** y **Término del intervalo DID**. ▪ Para mapear un intervalo de números, especifique los números iniciales y finales que definen el intervalo. ▪ DID numbers can begin with a “+” character.
Tipo Destino	Seleccione de entre los siguientes tipos de destinos internos. Si no aparece un tipo de destino, no hay anexos internos de ese tipo configurados en el sistema: ▪ OPERATOR (OPERADORA) ▪ CONTESTADORA_AUTOMÁTICA ▪ GRUPO_DE_ENVÍO ▪ GRUPO_DE_BÚSQUEDA ▪ B_ACD (Anexo de servicios ACD básico)

Campo	Descripción
Destino	Si selecciona CONTESTADORA_AUTOMÁTICA, GRUPO_DE_BÚSQUEDA,GRUPO_DE_ENVÍO ó B_ACD como tipo de destino, seleccione el anexo o grupo adecuado de la lista que está configurada en su sistema. Si selecciona Operadora como el tipo de destino, especifique manualmente el anexo que se va a utilizar para la Operadora del sitio.

Plan de numeración saliente

Esta ventana aparece cuando se selecciona **Configurar** > **Telefonía** > **Plan de numeración** > **Saliente** en la barra de funciones.

NOTA Debe estar activado el acceso a Telnet para poder configurar las funciones del plan de numeración.

La ventana del Plan de numeración saliente tiene las siguientes fichas:

- **Administración de llamadas salientes**
- **Grupos de enlaces PSTN**
- **ID de quien llama**

Administración de llamadas salientes

En la ficha Administración de llamas salientes, usted puede:

- **Seleccione una Localización del plan de numeración**
- **Definición del código de acceso por defecto y Límite de tiempo de recolección de dígitos**
- **Configurar números salientes**
- **Agregar o editar un número saliente**

Seleccione una Localización del plan de numeración

En el menú Localización del plan de numeración, seleccione una de lo siguientes opciones:

- Una plantilla del plan de numeración incorporado para una localización específica, por ejemplo, Plantilla: Australia o Plantilla: Norteamérica.

  Las siguientes localizaciones tienen plantillas incorporadas: Argentina, Australia, Austria, Bélgica, Brasil, Chile, China, Colombia, Francia, Alemania, Indonesia, Irlanda, Italia, Japón, Malasia, México, Holanda (6 dígitos ó 7 dígitos), Nueva Zelanda, Norteamérica (7 dígitos y 10 dígitos), Noruega, Filipinas, Singapur, Eslovenia, España, Suiza, RU, Taiwán, Tailandia y Venezuela.

  Para Norteamérica, se entregan plantillas de planes de discado con 7 dígitos y con 10 dígitos, para que no se tengan que editar manualmente el plan de numeración para el discado local. En forma similar, plantillas de 6 y 7 dígitos se entregan para Holanda.

- Definición de una nueva localización (se crea un plan de numeración nuevo y vacío).
- Una plantilla personalizada basada en una de las plantillas por defecto con modificaciones o una plantilla personalizada importada.

Una vez que seleccione una localización del plan de numeración, la ficha se actualiza para mostrar los números salientes definidos en la localización seleccionada o, si seleccionó **Definir nueva localización**, se borran todos los números salientes.

Una vez que se haya agregado o modificado alguno de los números salientes de la plantilla por defecto para una localización, se crea un nuevo plan de numeración con sus cambios, dejando la plantilla original intacta.

Cuando se aplica por primera vez una plantilla de plan de numeración saliente, si dicha plantilla contiene algún número bloqueado, se le preguntará si desea activar o desactivar globalmente el bloqueo de llamadas en todos los teléfonos de usuarios. Esta opción global aparece sólo durante la configuración inicial del plan de numeración. Si se agregan o eliminan números bloqueados después que se aplique la plantilla, esta opción global de activar/desactivar no está disponible. El bloqueo de llamadas en los teléfonos agregados después que se aplique la plantilla del plan de numeración debe configurarse en forma manual en la ficha Anexos de usuarios de la ventana Voz.

Para obtener más información, consulte **Plantillas de plan de numeración, página 480**.

Definición del código de acceso por defecto y Límite de tiempo de recolección de dígitos

Un código de acceso es un número de un solo dígito que los usuarios telefónicos utilizan para hacer llamadas externas. En el campo **Código de acceso**, especifique un solo dígito, de 0 a 9 o utilice el valor por defecto, 9. Esto define el código de acceso por defecto.

Si se cambia el Código de acceso por defecto para un plan de numeración existente, Configuration Assistant muestra un diálogo preguntando si se desea aplicar el código de acceso por defecto a todos los números salientes. Seleccione **Sí** para actualizar todos los números salientes del plan de numeración existente.

En el campo **Límite de tiempo de recolección de dígitos**, especifique la cantidad de segundos (de 2 a 120) que debe esperarse la entrada del usuario cuando éste marque o utilice el valor por defecto de 5.

Configurar números salientes

PRECAUCIÓN Todos los cambios a la configuración del plan de numeración para los números salientes deben probarse. Los errores en la configuración del plan de numeración puede hacer que los clientes no puedan hacer llamadas.

Cisco recomienda enfáticamente que se utilice un teléfono IP real para probar el plan de numeración saliente después que se haya aplicado la configuración. CCA revisa y busca conflictos dentro del UC500, pero revisar la compatibilidad con el proveedor de telecomunicaciones está fuera del ámbito de CCA.

Por ejemplo, algunos proveedores de telecomunicaciones de Norteamérica exigen que el prefijo de acceso PSTN se envíe a CO, mientras que otros proveedores exigen que el código de acceso se elimine.

Es posible que necesite **Agregar o editar un número saliente** en el plan de numeración para:

- **Cambiar permisos para ciertos tipos de llamadas.**

  Evitar que los usuarios marquen ciertos números (bloqueo de llamadas). El bloqueo de llamadas evita las llamadas a números restringidos. Cuando un usuario intente hacer una llamada a un número bloqueado, se reproduce un tono de ocupado rápido durante unos 10 segundos. La llamada se termina y la línea vuelve a quedar disponible. El bloqueo de llamadas puede

activarse y desactivarse en todos los tipos de teléfonos, excepto los teléfonos SIP. El bloqueo de llamadas se controla en forma separadaa de los permisos del usuario y debe activarse teléfono a teléfono en la ventana Más opciones de la ficha Usuarios en la ventana Voz. Para obtener más información, consulte **Ejemplo de bloqueo de llamadas, página 480**.

Los permisos de llamadas y números restringidos del plan de numeración no se aplican a las línea de enlace CO (oficina central). Las opciones **Bloquear llamadas restringidas** y **Permisos** no están disponibles para las líneas CO.

El Asistente de configuración de telefonía no activa globalmente el bloqueo de llamadas para los teléfonos de usuarios cuando se aplica la plantilla del plan de numeración. Una vez que el asistente termine, se debe configurar manualmente el bloqueo de llamadas en cada teléfono.

- **Permita que los usuarios telefónicos realicen llamadas a números específicos que estén fuera de sus permisos normales**. Por ejemplo, los usuarios telefónicos autorizados a marcar números National Plus también pueden necesitar poder llamar a un número internacional para comunicarse con la casa matriz. En ese caso, se puede agregar un número saliente específico para ese objetivo y configurar sus permisos como National Plus.
- **Edite la Lista de enlaces para rutear llamadas hacia el enlace adecuado en orden de preferencia**. Por ejemplo, si selecciona Sólo PSTN para la Lista de enlace para los números Locales y Local Plus, todas las llamadas locales y de Local Plus y de emergencia se rutearán hacia los enlaces PSTN. Si selecciona SIP luego PSTN como el Tipo de enlace para llamadas Internacionales e International Plus, éstas se rutean hacia los enlaces SIP disponibles primero (ya que están libres), con reserva hacia los enlaces PSTN.

Agregar o editar un número saliente

Para agregar un número saliente, haga clic en **Agregar número** para insertar una nueva fila en la tabla, realice la configuración como se describe en la siguiente tabla, luego, haga clic en **Aceptar** o **Aplicar**.

Campo	Descripción
Permisos	Nivel de permisos para el número saliente. También se puede definir patrones para el bloqueo de llamadas. Cada número saliente tiene un nivel de permisos. El nivel de permisos corresponde a la configuración de **Permisos** y **Bloquear llamadas restringidas** que se configuren en cada teléfono. Los niveles de permisos son acumulativos, como se indica a continuación: ▪ **Bloqueado**. Número restringido. Cuando se activa **Bloquear números restringidos** para un teléfono, se bloquean las llamadas a estos números. ▪ **Emergencia**. Número saliente para las llamadas a servicios de emergencia. Se incluyen los números de emergencia en todos los niveles de permisos. ▪ **Números sin cargo**. Número saliente para llamadas sin cargo que se incluye en todos los niveles de permisos. ▪ **Local**. Incluye llamadas de emergencia, sin cargo y locales. ▪ **Local más**. Incluye llamadas de emergencia, sin cargo, locales y Local Plus. ▪ **Nacional** Incluye llamadas de emergencia, sin cargo, locales, Local Plus y Nacionales. ▪ **Nacional Plus**. Nacional Incluye llamadas de emergencia, sin cargo, locales, Nacionales y National Plus. ▪ **Internacional**. Nacional Incluye llamadas de emergencia, sin cargo, locales, Nacionales, National Plus e Internacionales. ▪ **International Plus**. Nacional Incluye llamadas de emergencia, sin cargo, locales, Nacionales, National Plus, Internacionales e International Plus. ▪ **Sin restricciones**. Incluye todos los niveles de permisos, excepto Bloqueados.

Campo	Descripción
Descripción	Descripción de la norma del número saliente. Para las llamadas bloqueadas, la descripción siempre es Número restringido y se muestra en forma automática.
Código de acceso	Código de acceso, si es necesario, para marcar el número saliente. En la mayoría de los casos, se tratará del código de acceso por defecto para llamadas externas. También se puede especificar un código de acceso diferente para un número saliente.
Comienza con	Número o patrón con que debe coincidir. ▪ El patrón debe ser único. ▪ Los números y patrones coinciden comenzando con el primer dígito. ▪ Un número que incluye el patrón, pero que no comienza con éste, no coincide. ▪ Cuando se especifica un patrón, una "x" coincide con cualquier dígito del 0 al 9. Una serie de números entre corchetes ([089]) coincide con alguno de los dígitos. ▪ También se puede especificar un intervalo. Por ejemplo, [2-9] coindice con cualquier dígito en el intervalo de 2 a 9.
Número de dígitos	Especifique la cantidad de dígitos del número marcado o seleccione **Variable**. La cantidad de dígitos no puede ser menor que el prefijo definido en el campo **Comienza con** y no puede ser mayor que 15.
Patrón de marcación	A medida que especifique patrones en el campo **Comienza con**, la columna **Patrón de marcación** de la tabla se actualiza y muestra el patrón de discado que coincide, incluyendo el código de acceso. La columna **Patron de marcación** es de sólo lectura.

Campo	Descripción
Prioridad de enlace	La configuración de prioridad de enlace le permite asignar prioridades al enlace saliente con el menor costo para un tipo dado de llamadas. Especifique una prioridad de enlace para el número saliente. Las alternativas incluyen **Sólo PSTN**, **Sólo SIP**, **PSTN luego SIP**, **SIP luego PSTN**, o **Ninguna**.
Configurar prioridad	*Opcional*. Haga clic en el botón **Configurar prioridad** para abrir el díalogo Detalles de lista de enlaces, donde se puede visualizar o editar la configuración de la lista de enlaces. Para editar la configuración de la lista de enlace: 1. Haga clic en la columna **Preferencia** que corresponda al enlace cuya prioridad se desee editar y seleccione una nueva prioridadm, desde 1 (la más alta) hasta 10 (la más baja). 2. Haga clic en **Agregar enlace** para agregar grupos de enlaces que estén configurados en el sistema y que no se agregaron a números salientes cuando se crearon. Cuando se crea un enlace, se puede seleccionar si se desea agregarlo a la lista de enlaces para todos los números salientes. Si no se selecciona agregarlo al momento de su creación, utilice esta opción para agregarlo a un número saliente. 3. Haga clic en **Eliminar enlace** para quitar enlaces de la lista (por ejemplo, se puede eliminar un enlace SIP si desea que todas las llamadas se ruteen por medio de los puertos conectados a la PSTN). 4. La función **Enviar código de acceso** controla si el código de acceso discado por el usuario se envía al enlace. Por defecto, Enviar código de acceso está configurado como No. Este campo no debe modificarse, a menos que así lo solicite el Prestador de servicios. 5. Haga clic en **Aceptar**.

Para editar un número saliente, ubique el número que desea editar, haga clic en la fila para seleccionarlo, realice los cambios y haga clic en **Aceptar**.

Para eliminar un número saliente, ubique el número que desea eliminar, haga clic en la fila para seleccionarlo, realice los cambios y haga clic en **Eliminar** y luego en **Aceptar**.

Ejemplo de bloqueo de llamadas

Para configurar el plan de numeración para que las llamadas a todos los números que comiencen con 1976 para el Plan de numeración para Norteamérica estén bloqueadas, siga estos pasos:

PASO 1 En la ventana Números salientes, haga clic en **Agregar número**.

PASO 2 En el menú **Permisos**, seleccione **Bloqueado** y especifique el código de acceso.

PASO 3 En el campo **Comienza con**, especifique 1976.

PASO 4 En la columna **Número de dígitos**, especifique 11.

PASO 5 La configuración de **Lista de enlace** y **Configurar prioridad** no se aplican a los números bloqueados.

PASO 6 Haga clic en **Aceptar**.

Una vez que se haya modificado el plan de numeración para agregar números bloqueados, se debe activar **Bloquear llamadas restringidas** en cada teléfono para el que se desee bloquear estos números. Para acceder a esta configuración, seleccione **Configurar** > **Telefonía** > **Usuarios y anexos** > **Usuarios y teléfonos**, seleccione la ficha Anexos de usuarios y luego, configure el bloqueo de llamadas para cada botón de línea Normal o Compartido en el teléfono.

Plantillas de plan de numeración

Por medio de las plantillas del plan de numeración, Configuration Assistant entrega soporte para personalizar el plan de numeración saliente para que cumpla con los requisitos específicos de la localización. En la ficha Administración saliente, usted puede:

- **Definir una nueva localización** que no esté basada en una plantilla existente. Para definir una nueva localización, seleccione **Definir nueva localización** en el menú Localizacion del plan de numeración. Ello crea una nueva y vacía localización del plan de numeración.
- **Importar una plantilla.** Cuando se importa una plantilla, ésta se copia en la ubicación que contiene las plantillas del plan de numeración incorporadas de Configuration Assistant. Posteriores inicios de Configuration Assistant muestran la nueva plantilla como una opción del menú Localización del plan de numeración. Para importar una plantilla, haga clic en **Importar plantilla**.
- **Exportar una nueva localización o una configuración existente como plantilla**. Cuando se exporte una plantilla, se solicitará especificar un

nombre único para ella. Se guarda en la misma ubicación que las plantillas del plan de numeración incorporadas a Configuration Assistant. Posteriores inicios de Configuration Assistant muestran la plantilla exportada en el menú Localización del plan de numeración de la ficha Administración de llamadas salientes. Para exportar una localización o configuración existente como nueva plantilla, haga clic en **Exportar como plantilla**.

- **Eliminar una localización**. Para eliminar una localización, seleccione **Eliminar localización** en el menú Localizacion del plan de numeración. Utilice las teclas de flecha del diálogo Eliminar plantilla de localización para desplazar las plantillas de localización disponibles a la lista de plantillas de localización eliminadas y, luego, haga clic en **Aceptar**. Haga clic en **Aceptar** de nuevo cuando se le solicite confirmar la eliminación.

Grupos de enlaces PSTN

Los grupos de enlaces PSTN entregan una forma para agrupar lógicamente puertos de voz en grupos de enlaces para permitir flexibilidad en la selección de puertos de voz para llamadas salientes.

NOTA El soporte de Ruteo de menor costo abordado en esta sección se refiere al proceso de seleccionar manualmente un enlace PSTN o SIP marcando un código de acceso definido previamente.

El Ruteo de menor costo se refiere a la capacidad de seleccionar el enlace saliente con el menor costo para un tipo específico de llamada.

Configuration Assistant entrega soporte para el Rueto de menor costo al dar la capacidad de:

- Configurar la prioridad del enlace para los números salientes
- Asignar un esquema de búsqueda para los puertos de voz dentro de un enlace
- Crear y administrar nuevos grupos de enlaces PSTN para formar agrupaciones lógicas de puertos de voz

Para crear un nuevo y personalizado grupo de enlace PSTN, seleccione la ficha Grupo de enlaces PSTN y haga clic **Agregar**. Consulte **Parámetros del Grupo de enlaces, página 485**.

ID de quien llama

Consulte estas secciones para ver detalles sobre cómo configurar la ID de quien llama:

- **Especifique el código de bloqueo por llamadas de la ID de quien llama**

- **Especifique la ID de quien llama por defecto que se va a mostrar para cada Grupo de enlaces PSTN**
- **Anulación de la ID de quien llama por defecto para anexos específicos**

Especifique el código de bloqueo por llamadas de la ID de quien llama

El **Código de bloqueo por llamadas de ID de quien llama** es un código de cuatro dígitos que los usuarios telefónicos pueden marcar antes de hacer una llamada. El código debe comenzar con un asterisco (por ejemplo, *111).

Los usuarios marcan el código antes de hacer cualquier llamada en la que no deseen que su número aparezca en el teléfono de la persona a quien llaman. El identificador de llamadas se envía, pero su presentación parámetro se establece en "restringida" para que el identificador de llamadas no se muestra.

Para configurar el código, especifique un número de 3 dígitos en el campo Código de bloqueo por llamadas de ID de quien llama y haga clic en **Aplicar** o **Aceptar**.

CCA inserta automáticamente el asterisco (*). Por ejemplo, si se especifica 222 como el código de bloqueo por llamadas, los usuarios telefónicos marcarán *222 para bloquear la visualización de su ID de quien llama para una llamada.

Especifique la ID de quien llama por defecto que se va a mostrar para cada Grupo de enlaces PSTN

El Número PSTN principal de ID de quien llama es el número de ID de quien llama que se muestra por defecto para todas las llamadas salientes desde un grupo de enlaces SIP o PSTN.

La ficha ID de quien llama muestra todos los grupos de enlaces PSTN o de enlaces SIP por defecto y personalizados que están configurados en el sistema, junto con el Número PSTN principal de ID de quien llama para cada grupo de enlaces. Por defecto, el Número PSTN principal de ID de quien llama utiliza el mismo número PSTN principal que se configuró cuando se creó el enlace.

Para modificar la ID de quien llama para un grupo de enlaces, siga estos pasos.

PASO 1 En la ficha ID de quien llama de la ventana Plan de numeración saliente, haga clic en un grupo de enlaces PSTN para seleccionarlo.

PASO 2 Haga clic en el campo **Número PSTN principal de ID de quien llama** para el grupo de enlaces PSTN seleccionado.

PASO 3 Especifique el número telefónico que se mostrará para la ID de quien llama. El número puede tener hasta 15dígitos. El número puede comenzar con un carácter "+".

PASO 4 Haga clic en **Aceptar** o **Aplicar**.

Se puede anular la ID de quien llama por defecto para anexos específicos. Consulte **Anulación de la ID de quien llama por defecto para anexos específicos, página 483**.

Anulación de la ID de quien llama por defecto para anexos específicos

Para anular la ID de quien llama por defecto para anexos específicos, siga estos pasos.

PASO 1 En la ficha ID de quien llama de la ventana Plan de numeración saliente, haga clic en un grupo de enlaces PSTN para seleccionarlo.

PASO 2 Haga clic en **Agregar**.

Aparece el diálogo Agregar ID de quien llama para anexos internos. Complete los campos de este diálogo como se describe en **Agregar ID de quien llama para los anexos internos, página 483**.

Se puede agregar hasta 14 entradas de anulación de ID.

PASO 3 Haga clic en **Aceptar** o **Aplicar**.

Para modificar la configuración existente de anulación de ID de quien llama, destaque la entrada de anulación de ID de quien llama y haga clic en **Modificar**.

Agregar ID de quien llama para los anexos internos

Esta ventana aparece cuando se selecciona un Grupo de enlaces PSTN en la ficha ID de quien llama de la ventana Plan de numeración saliente y se hace clic en **Agregar** o **Modificar**.

Configure la ID de quien llama para anexos internos como se describe a continuación y haga clic en **Aceptar**. Se puede agregar hasta 14 entradas de anulación de ID. Al especificar un intervalo de anexos internos que se mapean a uno o más números de ID de quien llama, se puede reducir el número de entradas necesarias.

Campo	Descripción
Número inicial de anexos internos **Número final de anexos internos**	Especifique los números iniciales y finales de los anexos internos para anular la ID de quien llama por defecto para un intervalo de números. Para anular la ID de quien llama por defecto para un solo anexo, especifique el mismo número de anexos en los campos Número inicial de anexos internos y Número final de anexos internos.
Número inicial de ID de quien llama **Número final de ID de quien llama**	Especifique los números iniciales y finales para anular la ID de quien llama por defecto para el intervalo de anexos internos especificado. Los números pueden empezar con un carácter "+", sin embargo, si el anterior "+" se utiliza para el número inicial, sino que también debe utilizarse para el número final. Si se está mapeando un intervalo de anexos internos hacia un intervalo de número de ID de quien llama, deben coincidir los dígitos finales. Por ejemplo, si se especifica 205 hasta 210 como los números iniciales y finales para los anexos internos, los números iniciales y finales de ID de quien llama deben terminar en -05 y en -10. Para un solo grupo de enlaces PSTN, los intervalos de anexos internos no pueden sobreponerse. Para anular la ID de quien llama por defecto para un solo anexo o para mostrar el número de ID de quien llama para un intervalo de anexos, especifique el mismo número en los campos Número inicial de ID de quien llama y Número final de ID de quien llama.

Ejemplos

Para anular la ID de quien llama por defecto para los anexos 205 hasta el 225 con los números de ID de quien llama desde 12229990005 hasta el 12229990005:

- Especifique 205 para el Número inicial del anexo interno.
- Especifique 225 para el Número final del anexo interno.
- Especifique 12229990005 para el Número inicial de ID de quien llama.
- Especifique 12229990025 para el Número final de ID de quien llama.

Para mostrar 12229991200 como la ID de quien llama para anexos internos 200 hasta el 230:

- Especifique 200 para el Número inicial del anexo interno.
- Especifique 230 para el Número final del anexo interno.
- Enter 12229991200 tanto para el Número inicial de ID de quien llama como para el Número final de ID de quien llama.

Para anular la ID de quien llama por defecto para el anexo 505 sólo con la ID de quien llama 12229991100:

- Especifique 5050 tanto para el Número inicial del anexo interno como para el Número final del anexo interno.
- Enter 12229991100 tanto para el Número inicial de ID de quien llama como para el Número final de ID de quien llama.

Parámetros del Grupo de enlaces

Esta ventana aparece cuando se hace clic en **Agregar** o **Modificar** en la ficha Grupo de enlaces PSTN de la ventana Plan de numeración saliente

Todos los puertos de voz se ubican inicialmente en grupos por defecto basados en su tipo de SKU. Por ejemplo, ALL_FXO o ALL-BRI. Estos grupos por defecto pueden modificarse.

Cuando se crea un nuevo grupo de enlaces PSTN, se le solicita seleccionar si desea agregar el nuevo enlace como opción para todos los números salientes o agregar manualmente el grupo de enlaces a números seleccionados, según sea necesario.

Cuando se crea un nuevo enlace SIP o un grupo de enlaces T1/E1, se le solicita especificare un número PSTN principal para estos enlaces. Se necesita este número PSTN principal para los grupos de enlaces que no están vacíos. Si se crea un grupo de enlaces, pero no se asignan puertos de voz como miembros, no es necesario tener un número PSTN principal. Si hay puertos de voz asignados a ese grupo de enlaces, sí es necesario.

Al crear o modificar un Grupo de enlaces PSTN, realice la configuración como se describe a continuación y haga clic en **Aceptar**.

Campo	Descripción
Grupo de enlaces	Nombre descriptivo para este grupo de enlaces.
Esquema de búsqueda	El esquema de búsqueda determina cómo se seleccionan los puertos de voz miembros para las llamadas salientes. Están disponibles las siguientes opciones: ▪ **secuencial**. Selecciona el puerto de voz con la más alta preferencia. ▪ **todos contra todos**. Selecciona el próximo puerto de vozs con ranuras de tiempo libres. ▪ **aleatorio**. Selecciona una ranura de tiempo en forma aleatoria. ▪ **desocupado más tiempo**. Selecciona el puerto de voz con la ranura de tiempo que está desocupada por más tiempo. ▪ **menos desocupado**. Selecciona el puerto de voz con la ranura de tiempo que está desocupada por menos tiempo.
Tipo de enlaces	Seleccione un tipo de enlace de la lista de tipos de enlaces disponibles en su sistema.

Campo	Descripción
Miembros del grupo de enlaces	Seleccione los miembros del grupo de enlaces de la lista de puertos de voz disponibles para el tipo de enlace seleccionado. Un puerto de voz puede pertenecer a sólo un grupo de enlaces PSTN. No se puede mezclar tipos diferentes de enlaces PSTN en un solo grupo de enlaces. Por ejemplo, un puerto FXO análogo no puede ser miembro de un grupo de enlaces que contenga puertos BRI de ISDN. Utilice las teclas de flecha **Hacia arriba** y **Hacia abajo** para volver a ordenar la lista de puertos de voz, si el esquema de búsqueda seleccionado es secuencial o del tipo todos contra todos.

16

Gestión del sitio

Se analizan los siguientes temas:

- **Administrador de múltiples sitios**
- **Máximo de llamadas (Control de admisión de llamadas)**

Administrador de múltiples sitios

Utilice el Administrador de múltiples sitios para configurar, administrar y monitorear hasta 5 sitios de clientes de SBCS de Cisco a través de una VPN de malla completa.

Esta función permite que los usuarios finales en los sitios conectados realicen llamadas entre sitios utilizando el discado abreviado y compartan datos por una conexión WAN segura. Las implementaciones de múltiples sitios están bien adaptadas para pequeñas empresas con hasta 5 ubicaciones.

Los modelos de implementación admitidos incluyen sitios de clientes con un solo UC500 ó con un UC500 detrás de un router seguro SR500 de Cisco para las funciones de seguridad avanzadas.

- **Requisitos y pautas de diseño de múltiples sitios**
- **Procedimientos de configuración de múltiples sitios**
- **Monitoreo del estado de múltiples sitios**
- **Funciones de voz admitidas en múltiples sitios**

Requisitos y pautas de diseño de múltiples sitios

Sólo las siguientes topologías de redes se admiten para los sitios de clientes individuales que sean miembros de una implementación de múltiples sitios. Cualquiera de estas topologías de sitios pueden combinarse mientras el número total de sitios sea igual o inferior a 5. Los sitios están configurados con una VPN de malla completa; es decir, cada sitio tiene un enlace directo a todos los demás sitios.

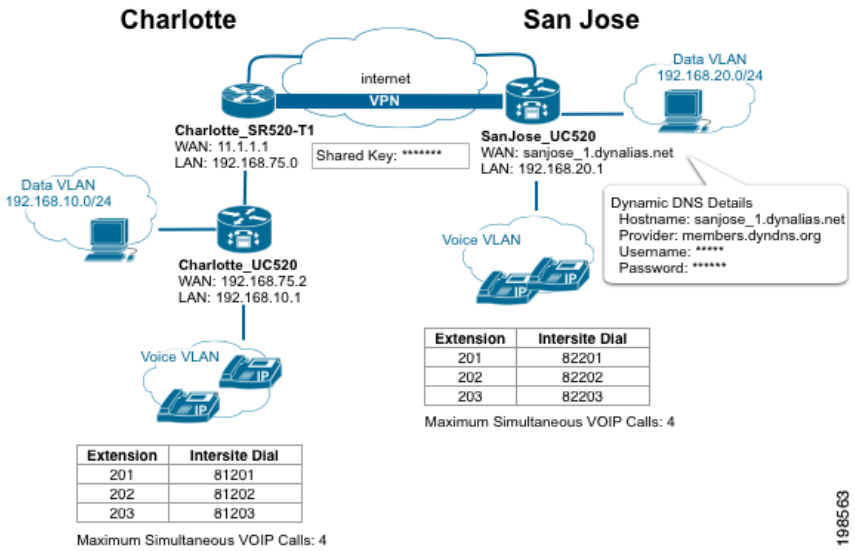
- Un solo UC500 conectado a la WAN.
- Un solo router seguro SR520-T1 combinado con un UC500. El SR520-T1 se conecta a la WAN y entrega funciones de seguridad avanzadas y el UC500 entrega voz y datos al sitio. En este tipo de implementación, la VLAN de datos debe ser única tanto para el SR500-T1 como para el UC500.

  Para la versión actual, sólo el router seguro modelo SR520-T1 se admite para ser utilizado en las implementaciones de múltiples sitios de SBCS de Cisco configuradas con CCA.

IMPORTANTE Cada sitio *debe* tener un UC500 para voz y datos. El Administrador de múltiples sitios no puede usarse para configurar ninguno de los siguientes tipos de implementación:

- Un router autónomo SR520-T1 como uno de los sitios
- Una VPN de sitio a sitio de sólo datos entre dos o más routers seguros SR500
- Un teléfono remoto detrás de un SR520-T1 sin un UC500

Este diagrama muedstra un simple ejemplo de una implementación con dos sitios que ilustra las topologías admitidas y algunos de los requisitos de diseño analizados en esta sección.



El ejemplo anterior ilstra estos elementos clave de la configuración de múltiples sitios:

- **Topología del sitio**. El sitio de Charlotte entrega un ejemplo de un sitio que tiene un UC500 detrás de un SR520-T1, mientras que el sitio de San José tiene sólo un UC500.
- **La dirección IP de la VLAN de datos debe ser única**. Debido a que las direcciones IP de la VLAN de datos deben ser únicas en todos los sitios para cualquier UC500 y también para cualquier SR520-T1, la IP de la VLAN de datos para el UC500 en el sitio Charlotte se define como 192.168.10.1/24, y la dirección IP para la VLAN de datos para el UC500 de San Jose se define como 192.168.20.1/24. La IP de la VLAN para el SR520-T1 en el sitio de Charlotte es 192.168.75.0/24 y no hay un SR520-T1 presente en el sitio de San Jose (de lo contrario, también sería necesaria una IP de VLAN de datos única para él).

- **Plan de numeración y numeración entre sitios**. Para esta configuración, hemos optado por utilizar un prefijo de marcación entre sitios de "8". La ID del sitio de Charlotte configurada como “1” y la ID del sitio de San Jose como "2". Como lo muestra el ejemplo, los usuarios telefónicos marcan el *Prefijo de discado entre sitios* + la *ID del sitio* + el *anexo* para llegar a otros sitios. Ambos sitios tienen su longitud de anexo definida como 3. Aunque no es necesario que los sitios utilicen la misma longitud de anexo, se recomienda para facilitar el uso y la configuración.
- **Se admiten direcciones IP estáticas o de WAN de DHCP**. El sitio de Charlotte usa una dirección IP de WAN estática, mientras que el sitio de San Jose está configurado para usar DHCP. Ya que se usa DHCP, se configura una DNS dinámica (DDNS) para el sitio de San Jose.
- **VPN de malla completa con autentificación por medio de clave previamente compartida**. Una clave global previamente compartida se configura en forma idéntica para cada sitio que entrega autentificación para el túnel VPN.
- **Control de Admisión de llamadas**. Ambos sitios se configuran para permitir un máximo de
  4 llamadas simultáneas en la WAN.

Esta table indica y describe los requisitos y pautas de diseño de múltiples sitios con mayor detalle.

IMPORTANTE La configuración fuera de banda existente no es admitida en el Administrador de múltiples sitios. Se debe eliminar la configuración fuera de banda existente para múltiples sitios antes que pueda usar el Administradorde múltiples sitios.

Elemento de configuración	Requisitos/Pautas recomendadas
Número de sitios	Hasta 5 sitios en una topología de malla completa.

Elemento de configuración	Requisitos/Pautas recomendadas
Número de túneles IPSec	Para las plataformas UC520 y UC540, cada sitio de clientes admite hasta 10 túneles de IPSec. Para las plataformas UC560, cada sitio de clientes admite hasta 20 túneles de IPSec. Ello incluye los túneles EZVPN, VPN sobre SSL, VPN de múltiples sitios y VPN de teléfonos SPA525G. Cuando un sitio es parte de una implementación de múltiples sitios, *N-1* de estos túneles VPN se utilizan para la VPN de malla completa y sitio a sitio, donde *N* es el número de sitios. Por ejemplo, si la implementación de múltiples sitios para una plataforma UC540 tiene 4 sitios, 3 túneles IPSec se utilizan para la VPN de malla completa y de sitio a sitio, dejando 7 túneles disponibles para EZVPN y/o vPN sobre SSL.
Firewall	Firewall basado en zonas (ZBF) de Cisco en el SR500 o política de CBAC basado en IOS de Cisco en el UC500. No se admiten firewalls de terceros.

Elemento de configuración	Requisitos/Pautas recomendadas
Direcciones de VLAN de datos	La dirección IP de la VLAN de datos para cada UC500 y SR520-T1 debe ser única en todos los sitios. Si cada sitio tiene valores por defecto de fábrica, se debe recordar de modificar la dirección por defecto de la VLAN de datos durante la configuración inicial de cada miembro del sitio adicional para asegurarse que sean única. Use el Asistente de configuración de telefonía para realizar la configuración inicial. Si uno de los sitios remotos tiene una dirección IP de la VLAN de datos que no sea única, se debe modificar su dirección de VLAN de datos. Para un sitio que no esté en su estado por defecto de fábrica, esto sólo puede hacerse por medio del Administrador de múltiples sitios. Luego de modificar la dirección IP de la VLAN de datos, se perderá conectividad al UC500 y se debe solicitar y obtener una nueva dirección IP del UC500. Para hacer esto, vaya a **Inicio** > **Ejecutar** en su PC y escriba **`cmd`** para abrir una ventana de comandos. Al solicitar el comando, especifique el comando **`ipconfig /renew`**.
Tipo de conexión WAN	Los sitios pueden utilizar ya sea direcciones IP estáticas o con DHCP con DDNS configurado. Para los sitios que utilizan DHCP para obtener una dirección IP en forma dinámica, debe utilizarse DDNS (Servicio de nombre de dominio dinámico) u otro método de registro de DNS para administrar las direcciones dinámicas. Cuando se configure DDNS, el nombre del proveedor DDNS, debe entregarse el nombre de host para cada sitio y la información de autentificación (nombre de usuario y contraseña) como parte de la configuración de la conexión de múltiples sitios. Consulte **Configuración de DDNS, página 509**. El nombre de host DDNS debe ser único para cada sitio.

Elemento de configuración	Requisitos/Pautas recomendadas
Servicio de hosting DDNS (DNS dinámico).	DDNS debe configuarse para los sitios con conexiones WAN de DHCP que son parte de una implementación de múltiples sitios. Los sitios que se configuren con una dirección IP estática no son necesarios para configurar DDNS. Estos servicios de hosting DDNS pueden seleccionarse desde la sección DDNS de HTTP en la ventana Conexión a Internet (**Configurar** > **Enrutamiento** > **Conexión a Internet> Modificar > configuración de conexión**). ▪ cgi.tzo.com ▪ dup.hn.org ▪ members.dyndns.org ▪ members.easydns.com ▪ www.dynx.cx ▪ www.justlinux.com ▪ www.zoneedit.com Las cuentas con estos proveedores de DDNS deben establecerse fuera de Configuration Assistant. **SUGERENCIA** Cisco recomienda que se actualice desde el paquete gratuito a un paquete pagado o premium del proveedor de DDNS. Por ejemplo, algunos paquetes gratuitos se diseñan para vencer por inactividad (por ejemplo, si la dirección IP no se actualiza en 30 días). La pérdida del soporte de DNS para un nombre de dominio significa que los túneles VPN quedan inoperables o no se activan, lo que ocasiona interrupciones en el servicio.
Morfología del tráfico/Calidad de servicio (QoS)	*Opcional*. Aunque esta configuración es opcional, se recomienda en forma enfática. Los sition que tengan un ancho de banda limitado también deberían dar forma al tráfico y configurar QoS para implementaciones en múltiples sitios.

Elemento de configuración	Requisitos/Pautas recomendadas
Códec	Se debe seleccionar G.711 ó G.729 como el códec que se usará para las llamadas entre los sitios. El códec G.729 ofrece mayor compresión, lo q se traduce en importantes ahorros de ancho de banda, pero puede ocasionar una peor calidad para algunos tipos de audio, como la Música en espera.
Control de Admisión de llamadas	*Opcional*. Configure el Máximo de llamadas (máximo de llamadas simultáneas) para asegurar la calidad de la voz para las llamadas de VoIP y entre sitios ayudando a evitar que la conexión a Internet esté sobre-utilizada. Configuration Assistant usa la configuración de QoS actualmente presente para el ancho de banda de subida, preferencia de códec, y la reserva de ancho de banda para los medios de voz para entregar recomendaciones para el control de admisión de llamadas.
Plan de discado	Especifique un **Prefijo de discado entre sitios** para hacer llamadas de sitio a sitio. Para discar a otro sitio, los usuarios telefónicos deben marcar: *Prefijo de discado entre sitios + ID del sitio + Anexo* Esta función permite flexibilidad en la asignación de anexos para los sitios. Los dígitos de prefijos que ya están en uso no están disponibles para ser seleccionados.
Longitud de anexo	Se recomienda, pero no es necesario, que todos los sitios de una configuración de múltiples sitios usen la misma longitud de anexo.

Elemento de configuración	Requisitos/Pautas recomendadas
Su nombre de host	Para evitar la confusión al seleccionar el nombre de host de los menús de Configuration Assistant, se recomienda que se definan los nombres de host del sistema para que sean únicos en todos los sitios. El nombre del host del sistema se muestra en los menús de selección de nombre de host y en las solicitudes del sistema de Configuration Assistant.

Procedimientos de configuración de múltiples sitios

Los temas de esta sección cubren los procedimientos de configuración para mútiples sitios para las configuraciones admititdas.

Si no se han configurado previamente conexiones de múltiples sitios en este UC500, la ventana inicial entrega una visión general de los pasos de configuración, con estas opciones:

- **Especicifar manualmente la configuración de múltiples sitios**. Seleccione esta opción para ir a la ficha de Configuración de múltiples sitios. Consulte **Agregar y configurar sitios, página 499**.
- **Importar archivo de configuración de múltiples sitios**. Seleccione esta opción para importar la configuración del sitio que se exportó previamente a un archivo de configuración de otro sitio. Consulte **Exportación e importación de sitios, página 512**.

NOTA Todos los procedimientos de configuración de múltiples sitios suponen que la PC que ejecuta Configuration Assistant está conectada a un puerto Ethernet en el UC500 y se ha obtenido una dirección IP de parte de éste. Cuando el UC500 está detrás de un router seguro SR520-T1, conéctese directamente al UC500 y use el DHCP para obtener una dirección IP desde el UC500.

- **Requisitos y pautas de diseño de múltiples sitios**
- **Requisitos previos para la configuración de múltiples sitios**
- **Agregar y configurar sitios**
- **Configuración de DDNS**
- **Configuración de Calidad de servicio (QoS)**

- **Máximo de llamadas (Control de admisión de llamadas)**
- **Exportación e importación de sitios**
- **Modificación de un sitio después de su configuración inicial**
- **Eliminación de un sitio**

Requisitos previos para la configuración de múltiples sitios

Deben cumplirse varios requisitos previos antes de poder configurar conexiones de múltiples sitios. Para obtener información más detallada, consulte **Funciones de voz admitidas en múltiples sitios, página 517**.

- Debe estabelecerse la configuración de datos y voz básica en el UC500, utilizando el Asistente de configuración de telefonía (recomendado para los sitios que se configuran con los valores por defecto de fábrica) o con Configuration Assistant en modo experto. Esto incluye:
  - Conexión a Internet
  - La dirección IP de la VLAN de datos para cada UC500 y SR520-T1 debe ser única en todos los sitios. Si no lo es, se puede modificar posteriormente por medio del Administrador de múltiples sitios.
  - Configuración de inicialización del sistema de voz, como el código de acceso por defecto para las llamadas externas (ficha **Configurar** > **Telefonía** > **Plan de numeración** > **Saliente** > **Gestión de llamadas salientes**).
  - Como mínimo, la telefonía local debe configurarse para llamadas dentro del sitio, preferentemente por medio del Asistente de configuración de telefonía.
- Si el router seguro SR500 es el dispositivo periférico (es decir, el UC500 en un sitio está detrás de un SR500), esta configuración debe realizarse:
  - Conexión WAN Si se utiliza un router seguro SR520-T1, se debe ejecutar la utilidad de conexión T1 antes de ejecutar el Asistente de configuración de telefonía.
  - El firewall y NAT están desactivados en el UC500. Cuando se ejecute el Asistente de configuración de telefonía, automáticamente se le pedirá hacer esto como parte de la configuración.
  - El UC500 tiene una dirección IP de WAN de 192.168.x.2 donde x se obtiene desde la VLAN75 de datos del SR500.

  - El SR500 puede enrutear hacia el UC500 (ruta estática simple a la VLAN1 de datos). Cuando se ejecuta el Asistente de configuración de telefonía, estas rutas se establecen en forma automática.
  - El SR500 debe tener una configuración de dirección única para toda la red para la VLAN75.
- Para los sitios que utilizan una conexión WAN de DHCP, se necesita la siguiente información para la configuración DDNS:
  - Nombre del proveedor de DDNS
  - Nombre de host único para cada sitio
  - Nombre de usuario y contraseña de la cuenta del proveedor de DDNS

Agregar y configurar sitios

Visión general

Si se está configurando conexiones para múltiples sitios con plataformas UC500 y SR500 con valores por defecto de fábrica, los pasos recomendados para configurar conexiones entre sitios son los siguientes:

1. Si cualquiera de los sitios usa un router seguro SR520-T1 como el dispositivo periférico, se *debe* ejecutar la Utilidad de conexión T1 primero (antes de ejecutar el Asistente de configuración de telefonía). Consulte la Guía de inicio rápido *Small Business Pro SR520-T1* de Cisco y la nota de aplicación de la *Configuración de router seguros UC500 y SR520-T1* para obtener más instrucciones.
2. En el primer sitio:
   a. Verifique que la configuración de datos y voz básica está establecida en el UC500.
   b. Inicie Configuration Assistant y configure Morfología de tráfico/Calidad de servicio, Máximo de llamadas (Control de admisión de llamadas) y configuración de DDNS, según sea necesario. Los sitios configurados con una conexión WAN de DHCP deben configurar DDNS para iniciar el Administrador de múltiples sitios.
   c. Inicie el Administrador de múltiples sitios (**Configurar** > **Telefonía** >**Administración de sitios**> **Administrador de múltiples sitios)** y realice la configuración global para múltiples sitios:
      - Clave previamente compartido para la autentificación del túnel VPN

- Prefijo para discado entre sitios
- Códec a utilizar para llamadas VoIP de sitio a sitio (G.711 ó G.729)

d. Realicela configuración de múltiples sitios para el primer sitio:
   - Nombre del sitio
   - Índice del sitio
   - Número de dígitos en los anexos.

e. Agregue los otros sitios remotos y realice la configuración básica para múltiples sitios:
   - Nombre del sitio
   - IP de WAN o Nombre de dominio completamente calificado (FQDN)
   - Direccionamiento interno (VLAN de datos para el UC500, ya sea que el sitio tenga un SR520-T1 o no)
   - Patrón de discado del sitio (número de ID del sitio y dígitos por anexo)

f. Exporte valores de la configuración de múltiples sitios configurados previamente y aplique la configuración.

3. En el segundo sitio y en cada uno de los sitios restantes (hasta 5 sitios, máximo).
   a. Verifique que la configuración de datos y voz básica está establecida en el UC500.
   b. Configure la Morfología de tráfico/QoS, Máximo de llamadas y del DDNS, según sea necesario.
   c. Inicie el Administrador de múltiples sitios e importe el archivo de configuración para múltiples sitios que se creó y exportí desde el primer sitio.
   d. Configure la misma clave previamente compartida en los sitios remotos.

Si se está configurando uno o más sitios existentes, los pasos son similares, excepto que en vez de utilizar el Asistente de configuración de telefonía, se establece la configuración en modo experto. Si se necesita cambiar la dirección IP por defecto de la VLAN para el SR520-T1 ó el UC500, se puede hacerlo por medio del Administrador de múltiples sitios al importar los datos del sitio.

Procedimientos

PASO 1 Verifique que se cumplen los requisitos descritos en **Requisitos previos para la configuración de múltiples sitios, página 498**.

PASO 2 Verifique que la PC que ejecuta Configuration Assistant esté conectado directamente al UC500 y que haya obtenido una dirección IP del UC500.

PASO 3 Inicie Configuration Assistant y conéctelo al primer sitio que se configure.

PASO 4 En la barra de funciones, seleccione **Configurar** > **Telefonía** > **Administración de sitios** >**Administrador de múltiples sitios**.

PASO 5 Seleccione la ficha Configuración de múltiples sitios.

PASO 6 Configure esta **Configuración global** para todos los sitios.

Configuración	Descripción
Clave previamente compartida para autentificación	Especifique una clave previamente compartida para autentificar sitios remotos. Utilice una clave previamente compartida que cumpla con los criterios de contraseña. From 8 to 127 characters can be entered; Spaces and “?” characters are not supported. Haga una marca en la casilla **Mostrar clave**para activar la visualización de la clave previamente compartida en texto plano. Haga una marca en la casilla **Permitir que se exporte la clave**para activar la exportación de la clave previamente compartida como texto plano en el archivo de configuración. **IMPORTANTE** La clave previamente compartida *debe* ser la misma para todos los sitios. Por defecto, la clave previamente compartida no se exporta en la configuración de múltiples sitios. Si se selecciona exportar la clave, se exporta como texto plano. Si no se exporta la clave previamente compartida, se debe volver a especificarla manualmente al importar los datos de configuración de múltiples sitios hacia otros sitios.

Configuración	Descripción
Códec	Códed preferido para las llamadas entre sitios. Seleccione uno: ▪ **G711**: El códec G711 es el preferido. ▪ **G729**: El códec G729 es el preferido.
Prefijo para discado entre sitios	Seleccione un prefijo de la lista desplegable. El sistema detecta los dígitos de prefijo que están en uso actualmente en el plan de numeración y sólo muestra las selecciones diponibles. Se trata del dígito de prefijo que los usuarios telefónicos deben marcar al hacer llamadas a otros sitios Para llamar a sitios remotos, los usuarios telefónicos marca el *Prefijo de discado entre sitios + ID del sitio + Anexo* Por ejemplo, si el dígito de prefijo para el discado entre sitios es 7 y un usuario en un sitio 1 desea llamar al anexo 307 del sitio 2, el usuario debe marcar 72037 para ese anexo.

PASO 7 Revisar y editar la configuración para el primer sitio. Se trata del sitio al que se conecta inicialmente.

Para comenzar a editar esta configuración, haga clic en **Editar**. Consulte **Configuracion del sitio, página 506** para obtener información adicional.

La siguiente información se lee y se muestra en el sitio al que se está conectado.

Configuración	Descripción
Dirección WAN	Sólo lectura. Dirección IP de la WAN de este sitio.
Dirección de VLAN de datos del UC500	Sólo lectura. Dirección IP de la VLAN de datos del UC500 para este sitio.
Máscara de subred de la VLAN de datos del UC500	Sólo lectura. Máscara de subred de la VLAN de datos del UC500 para este sitio.
Dirección de VLAN de datos del SR500	Sólo lectura. Dirección IP de la VLAN de datos del SR520-T1, si un SR520-T1 es parte del sitio del cliente.
Máscara de subred de la VLAN de datos del SR500	Sólo lectura. Máscara de subred de la VLAN de datos del SR520-T1, si un SR520-T1 es parte del sitio del cliente.
Patrón de discado del sitio	Campo de sólo lectura que muestra el patrón que los miembros del sitio marcan al hacer llamadas de sitio a sitio sobre la WAN.
Conectado a este sitio Haga clic en **Mostrar opciones de configuración adicionales** para ver el estado (ya sea **Configurado** o **No configurado**) de las configuraciones adicionales que podría ser necesario realizar para este sitio.	

Configuración	Descripción
DDNS	*Opcional*. Configuración de DNS dinámica. Indica si DDNS está configurado para este sitio o no. Si DDNS no está configurada y se está utilizando DHCP, se debe configurarla antes de poder iniciar el Administrador de múltiples sitios. Haga clic en el enlace **Configurado** o **No configurado** para abrir la ventana de Conexión a Internet, donde se puede modificar esta configuración. Consulte **Configuración de DDNS, página 509**.
Morfolofía de tráfico WAN	*Opcional, pero recomendado enfáticamente.* Indica si la configuración de Morfología de tráfico y Calidad de servicio (QoS) se ha configurado para el sitio. Aunque esta configuración es opcional, se recomienda enfáticamente para todos los sitios y, especialmente, sitio con ancho de banda limitado. Esto especifica la manipulación preferencia para el tráfico de voz sobre datos cuando es necesario. Haga clic en el enlace **Configurado** o **No configurado** para abrir la ventana de Conexión a Internet, donde se puede modificar esta configuración. Consulte **Configuración de Calidad de servicio (QoS), página 510**.
Control de Admisión de llamadas	Indica si está configurado Control de admisión de llamadas (CAC) para este sitio o no. La configuración de control de admisión de llamadas determina el número máximo de llamadas simultáneas para un sitio. Si no se configura CAC, seleccione **Configurar** > **Telefonía** > **Máximo de llamadas** en la barra de funciones para acceder a las opciones de configuración de acceso. Consulte **Máximo de llamadas (Control de admisión de llamadas), página 518**.

PASO 8 Una vez que se haya revisado y configurado para el primer sitio, haga clic en **Agregar sitio** y realice la configuración para el resto de los sitios que son parte de la implementación.

Consulte Configuracion del sitio, página 506.

PASO 9 Cuando haya finalizado de agregar y configurar todos los sitios remotos, haga clic en **Aplicar**.

El botón **Aplicar** está desactivado (gris pálido) si cualquiera de las configuraciones necesarias no está terminada (por ejemplo, clave previamente compartida).

Una vez que los cambios se aplican con éxito, el botón **Exportar archivo de configuración de múltiples sitios** queda activo.

PASO 10 Haga clic en **Exportar archivo de configuración de múltiples sitios**.

El botón **Exportar archivo de configuración de múltiples sitios** no está disponible (gris pálido) hasta que se haya aplicado con éxito la configuración.

PASO 11 Guarde el archivo de configuración en su PC. Se puede utilizar el nombre por defecto del archivo o especifique uno diferente.

IMPORTANTE No edite el archivo de configuración XML. Cualquier cambio a la configuración de múltiples sitios que se exporte debe hacerse por medio del Administrador de múltiples sitios e importarse nuevamente a cualquier sitio que sea parte de la configuración. Consulte Exportación de sitios, página 512.

PASO 12 Haga clic en **Aceptar**.

PASO 13 Guarde sus cambios a la configuración de inicio en todos los dispositovos del sitio del cliente:

- Haga clic en **Configurar** > **Guardar configuración**, o
- Haga clic en **Guardar** cuando se le solicite guardar la configuración antes de salir de Configuration Assistant.

PASO 14 Importe el archivo de configuración de múltiples sitios que acaba de exportar a cada uno de los otros sitios utilizando los procedimientos descritos en Importación de sitios, página 513.

Una vez que se importa y aplica la configuración entre todos los sitios remotos, comenzarán a activarse los túneles de VPN.

Se puede demorar hasta tres (3) minutos para que se establezcan los túneles de VPN.

Para activar manualmente los túneles IPSec, seleccione la ficha Estado de múltiples sitios y haga clic en **Conectar a todos los sitios**.

Configuracion del sitio

La ventana Configuración del sitio aparece cuando se

- Hace clic en **Agregar sitio** en la ventana Administrador de múltiples sitios.
- Hace clic en **Editar** (icono de Lápiz) en la ventana Administrador de múltiples sitios para editar la configuración para cualquiera de los sitios.

Agrega o modifica la configuración del sitio como se describe en esta tabla, luego se hace clic en **Aceptar** para volver al Administrador de múltiples sitios.

Los cambios realizados a la configuración del sitio ocasionará que se rechacen las llamadas y se interrumpa el tráfico de datos durante la re-configuración.

Configuración	Descripción
Información del sitio	
Nombre del sitio	Nombre descriptivo para este sitio.
Dirección IP o Dominio de WAN	Dirección IP pública (si se utilizan direcciones IP estáticas) o nombre del dominio completamente calificado para el sitio (si se utiliza DDNS).
Direcciones internas Si está directamente conectado a este sitio, los datos de Direcciones internas se leen desde la configuración actual del dispositivo. No se puede modificar la dirección IP de la VLAN para el UC500 ó el SR520-T1, pero si se hace, se muestra un diálogo de advertencia. ▪ Se le solicitará verificar u obtener nuevamente una dirección IP en su PC antes de reiniicar Configuration Assistant y volver a conectars al sitio del cliente. ▪ No se aplica otra configuración de múltiples sitios durante este cambio. Se debe volver a visitiar el Administrador de múltiples sitios y configurar o volver a importar su configuración de mútiples sitios una vez que se ha actualizado la VLAN.	
Dirección IP de VLAN de datos del UC500	Dirección IP de la VLAN de datos del UC500. Por ejemplo, 182.168.30.5.
Máscara de red de VLAN de datos del UC500	Máscara de subred para la VLAN de datos del UC500. Por ejemplo, 255.255.255.0. Si está directamente conectado a este sitio, esta información se lee desde la configuración actual del dispositivo.
El sitio usa el SR500 como dispositivo WAN	Marque esta opción si el UC500 está detrás de un router seguro SR520-T1.
Dirección de red de la VLAN de datos del SR500	Dirección IP de la VLAN de datos del SR520-T1. Si está directamente conectado a este sitio, esta información se lee desde la configuración actual del dispositivo.

Configuración	Descripción
Máscara de red de VLAN de datos del SR500	Máscara de subred para la VLAN de datos del SR520-T1. Si está directamente conectado a este sitio, esta información se lee desde la configuración actual del dispositivo.
Patrón de discado del sitio	
Prefijo para discado entre sitios	Este campo de sólo lectura muestra el prefijo de dígito único configurado actualmente para el discado de sitio a sitio. Es una configuración global para todos los sitios.
Dígitos por anexo	Número de dígitos utilizados para anexos internos (es decir, longitud de anexos).
Identificador del sitio	Especifique un número entre 1 y 5 que identifique este sitio. Es la ID del sitio utilizada para el discado entre sitios. Para marcar a este sitio, los usuarios telefónicos en sitios remotos deben usar este formato: *Prefijo de discado entre sitios + ID del sitio + Anexo* Por ejemplo, si el dígito de prefijo para el discado entre sitios es 7 y un usuario en un sitio 1 desea llamar al anexo 307 del sitio 2, se debe marcar 72037 para ese anexo.
Patrón de discado resultante	El campo de sólo lectura muestra el patrón de discado del sitio, basado en los valores configurados actualmente para el prefijo de discado entre sitios, el identificador del sitio y el número de dígitos por anexo.

Configuración de DDNS

DDNA sólo se exige para sitios que utilizan DHCP para obtener una dirección IP de WAN o sitios que usan PPoE con negociación de direcciones IP.

Procedimiento

PASO 1 Seleccione **Configurar** > **Enrutamiento** > **Conexión a Internet** y abra la ventana Modificar conexión a Internet.

PASO 2 En la sección **DDNS de HTTP** de la ventana Modificar conexión a Internet, complete esta configuración:

Campo	Descripción
Proveedor	Seleccione un proveedor de DDNS del menú desplegable. La cuenta con el proveedor de DDNS debe establecerse fuera de Configuration Assistant.
Su nombre de host	Nombre de host único para este sitio, obtenido de su proveedor de DDNS. Por lo general, un nombre de dominio completamente calificado (FQDN), por ejemplo, mihost.midominio.net, puede ser diferente para algunos servicios de DDNS. Debe registrarse el nombre de host. Configuration Assistant no valida este campo. Asegúrese que se haya especificado el nombre de host exactamente como lo especifica su proveedor de DDNS. Si está configurando una implementación de múltiples sitios, cada sitio debe tener un nombre de host DDNS único.
Nombre de usuario	Nombre de usuario de la cuenta, obtenido de su proveedor de DDNS.
Contraseña/ Confirmar contraseña	Contraseña de la cuenta, obtenida de su proveedor de DDNS. Especifique de nuevo la contraseña para confirmarla.

PASO 3 Haga clic en **Aceptar**.

PASO 4 Verifique que el cambio de configuración del sitio activó una actualización DNS con el proveedor de DDNS.

Configuración de Calidad de servicio (QoS)

La configuración de Calidad de servicio (QoS) para implementaciones de múltiples sitios permiten:

- Activar la morfología de tráfico
- Especificar el monto de ancho de banda de carga disponible para un sitio
- Especificar el porcentaje de ancho de banda de WAN disponible que se asigna para el tráfico de VoIP cuando está presente en la red
- Utilizar Control de admisión de llamadas (CAC) para asegurar que el conteo de llamdas no puede superar la asignación del ancho de banda para evitar la degradación.

Cuando QoS se activa y configura:

- Se entrega prioridad para el tráfico de red, hasta el porcentaje de ancho de banda de WAN disponible especificado. Cuando el tráfico de voz supera este porcentaje, se observará la degradación de audio para todas las llamadas de VoIP.
- El resto del ancho de banda de WAN disponible se utiliza para todo el otro tráfico de la red.
- Si no hay tráfico de voz presente en la red, todo el ancho de banda disponible puede utilizarse para tráfico de datos.

Pautas importantes

Estas pautas importantes se aplican a la configuración de QoS:

- Realice la configuración de QoS antes de configurar el Máximo de llamadas para que Configuration Assistant pueda determinar la configuración recomendada para CAC.
- La configuración de QoS es opcional, pero se recomienda enfáticamente. Por defecto, está desactivada.
- QoS debe configurarse en forma separada para cada sitio. No es parte de la configuración de múltiples sitios que se exporta por medio del Administrador de múltiples sitios.

- QoS siempre se configura en el dispositivo que está conectado a Internet:
  - Si el UC500 se conecta directamente a la WAN, configure QoS en el UC500.
  - Si el UC500 está detrás de un SR520-T1, configure QoS en el SR520-T1.
- Siempre especifique el ancho de banda real de subida para el sitio, según se determine con una prueba de velocidad de conexión confiable o con la Velocidad de información comprometida (CIR) en el Acuerdo de nivel de servicio (SLA) para el proveedor de servicio de Internet.

  Si los resultados de CIR y de la prueba de velocidad de conexión no están disponibles, especifique un ancho de banda de subida que sea aproximadamente el 80% del ancho de banda de subida publicitado por el proveedor de servicio de Internet.

  Si se aplica un ancho de banda que es mayor q las velocidades experimentadas, se puede ocasionar degradación del audio.

Procedimientos

PASO 1 Navegue hasta **Configurar** > **Enrutamiento** > **Conexión a Internet**.

PASO 2 En el menú **Nombre de host**, seleccione el nombre de host del dispositivo que esté contectado a Internet (ya sea, el UC500 ó un SR520-T1).

PASO 3 Haga clic sobre una conexión para seleccionarlo.

PASO 4 Haga clic en **Modificar**.

PASO 5 En la ventana Modificar conexión a Internet, haga clic en la ficha Morfología de tráfico.

PASO 6 Haga clic en la casilla **Morfología de tráfico** para activar la morfología del tráfico.

PASO 7 En el campo **Ancho de banda de subida [kbps]**, especifique el ancho de banda real de subida para el sitio, según lo dtermine una prueba de velocidad de conexión o la CIR (Velocidad de información comprometida) especificada en el SLA del proveedor de servicios. Por ejemplo, si la velocidad de carga es de 1,9 Mbps, especifique 1800 para el ancho de banda de subida.

Los valores varían entre 384 kbps y 100000 kbps.

Si no están disponibles los resultados de una prueba de velocidad, especifique un valor en kbps que sea el 80% del ancho de banda de subida publicitado por el ISP.

PASO 8 En el campo **Reserva de medios** , utilice la barra deslizante para especificar la proporción de ancho de banda disponible que se garantiza para los medios de voz si está presente en la red. Lo valores válidos varían entre 1 y 95 por ciento (el 5 por ciento restante cubre las señalizaciones y otros aspectos). Por defecto es 50%.

PASO 9 Haga clic en **Aceptar** o **Aplicar**.

PASO 10 Guarde la configuración (**Configurar** > **Guardar configuración**).

Exportación e importación de sitios

Una vez que se ha configurado la conexión para cada sitio, se exportan esta configuración a un archivo XML que puede importarse hacia cada uno de los otros sitios.

Exportación de sitios

Para cada sitio, se exporta la siguiente configuración:

- Nombre e índice del sitio
- Prefijo de discado entre sitios y número de dígitos en anexos
- Dirección IP pública o nombre de host del sitio
- Dirección IP y máscara de subred de la LAN de datos para el dispositivo periférico de la red (SR500 ó UC500)
- Dirección IP y máscara de subred del UC500, si está detrás de un router seguro SR500

IMPORTANTE Por motivos de seguridad, la **Clave previamente compartida** para la autentificación del sitio *no* se incluye en el archivo de la configuración exportada por defecto.

- Si no se exporta la clave previamente compartida en el archivo de configuración, se debe volver a ingresarla manualmente para cada sitio.

- Se puede incluir la clave previamente compartida en los datos exportados del sitio. La clave previamente compartida se exporta como texto plano, lo que es menos seguro.

No edite ni elimine ninguna de las configuraciones en este archivo XML. Cualquier cambio a la configuración de múltiples sitios debe realizarse a través de Configuration Assistant.

Para exportar la configuración de conexión de múltiples sitios:

PASO 1 Haga clic en **Exportar archivo de configuración de múltiples sitios.**

PASO 2 Guarde el archivo de configuración en la PC que ejecuta Configuration Assistant.

Importación de sitios

Para importar la configuración de conexión de múltiples sitios:

PASO 1 Conecte la PC que ejecuta Configuration Assistant directamente a un puerto de LAN en el UC500 para el sitio y asegúrese que la PC haya obtenido una dirección IP desde el UC500.

PASO 2 Inicie Configuration Assistant y conéctese al sitio.

PASO 3 Seleccione **Configurar** > **Telefonía** > **Administración del sitio** > **Administrador de múltiples sitios** de la barra de funciones para abrir el Administrador de múltiples sitios.

PASO 4 Si no se han configurado previamente conexiones de múltiples sitios, haga clic en el botón **Importar configuración de conexión de múltiples sitios** en la página que inicialmente se muestra para el Administrador de múltiples sitios.

Si se están importando configuraciones nuevamente, haga clic en **Importar sitio** desde la ventana Administrador de múltiples sitios.

PASO 5 Navegue hasa la ubicación del archivo de configuración que se exportó previamente y haga clic en **Aceptar**.

PASO 6 Seleccione el sitio que se va a importar y haga clic en **Aceptar**.

PASO 7 Si la configuración del sitio no coincide con la configuración actual del sitio, Configuration Assistant detecta las diferencias en la configuración y pregunta si se desea actualizar la configuración.

Si la dirección IP de la LAN de datos debe configurarse nuevamente en el UC500, se perderá la conectividad con Configuration Assistant y debe volver a conectarse con la nueva dirección IP.

Modificación de un sitio después de su configuración inicial

Se puede modificar la configuración del sitio después de la configuración inicial, pero si se hace, se debe:

- Exportar la nueva configuración.
- Importar la nueva configuración en todos los sitios.

Eliminación de un sitio

Para eliminar un sitio de la configuración de múltiples sitios, siga estos pasos.

PASO 1 Inicie Configuration Assistant y seleccione **Configurar** > **Telefonía** > **Administración del sitio** > **Administrador de múltiples sitios**.

PASO 2 En la ventana Administrador de múltiples sitios, seleccione la ficha Configuración de múltiples sitios.

PASO 3 Ubique el sitio que desea eliminar y haga clic en **Eliminar**.

PASO 4 Haga clic en **Aceptar** para confirmar esta acción.

PASO 5 Haga clic en **Aceptar** o **Aplicar**.

Para eliminar toda la configuración de múltiples sitios del dispositivo al que se está conectado, siga estos pasos:

PASO 1 Inicie Configuration Assistant y seleccione **Configurar** > **Telefonía** > **Administración del sitio** > **Administrador de múltiples sitios**.

PASO 2 En la ventana Administrador de múltiples sitios, seleccione la ficha Configuración de múltiples sitios.

PASO 3 Haga clic en **Eliminar configuración de múltiples sitios**. Esta opción se ubica en la esquina inferior derecha de la ventana Administrador de múltiples sitios. La opción **Elliminar configuración de múltiples sitios** sólo está disponible si el

Administrador de múltiples sitios detecta una configuración existente (es decir, una configuración se aplicó con éxito al menos una vez).

PASO 4 Haga clic en **Aceptar** cuando se le pregunte si desea eliminar toda la configuración de múltiples sitios.

Cuando se hace clic en **Aceptar**, toda la configuración de múltiples sitios existente se elimina completamente del dispositivo. La ventana Administrador de múltiples sitios se actualiza para mostrar la página inicial por defecto sin ninguna configuración.

Monitoreo del estado de múltiples sitios

Para monitorear las conexiones de túnel de VPN y ver la información de diagnóstico:

- Seleccione **Monitorear** > **Estado de múltiples sitios** en la barra de herramientas, o
- Haga clic en la ficha Estado de múltiples sitios en el Administrador de múltiples sitios.

El monitor del Estado de múltiples sitios tiene las siguientes áreas:

- **Resumen del estado del túnel VPN**
- **Detalles del estado del túnel VPN**

Resumen del estado del túnel VPN

La sección del Resumen del estado del túnel VPN muestra el estado de cada conexión de túnel VPN entre todos los sitios de la implementación. Si la configuración de varios sitios todavía no ha sido importado y se aplica a un sitio, el texto "Configuración del sitio No se ha aplicado"en la pantalla.

Haga clic en **Conectar a todos los sitios** para activar manualmente los túneles VPN entre todos los sitios.

Detalles del estado del túnel VPN

El área **Detalles del estado del túnel VPN** muestra la salida del comando **mostrar detalles de la sesión de cifrado**. Este comando muestra todas las sesiones activas de la Red privada virtual (VPN) y el IKE (Intercambio de claves por Internet) y SA (asociaciones de seguridad) de IPSec para cada sesión de VPN.

Fíjse en estas línea de la salida de ejemplo:

- **Estado de la sesión**. Se muestra el estado del túnel. Cuando el túnel se está activando, su estado es INACTIVO, NEGOCIANDO. Cuando el túnel está activo, el estado puede ser ACTIVO, ACTIVO SIN IKE o ACTIVO DETENIDO. Si el estado de la sesión es INACTIVO, el túnel no existe.
- **FLUJO IPSEC**. Una imagen instantánea del flujo de tráfico protegiso por IPSec. Las direcciones IP corresponden a las direcciones IP de la VLAN de datos y máscaras de subred configuradas para el UC 500 y el SR 500.

```
Estado actual de la sesión de cifrado

Código: C - Modo de configuración de IKE, D - Detección de pares muertos
K - Paquetes de actividad (Keepalives), N - NAT-traversal, T -
Encapsulamiento cTCP
X - Autentificación extendida IKE, F - Fragmentación IKE

Interfaz: Serie 1/0:1
-->Estado de la sesión: ACTIVA, SIN IKE
Par: Puerto 10.130.2.2 500 fvrf: (ninguno) ivrf: (ninguno)
      Desc: (ninguno)
      Phase1_id: (ninguno)
--> FLUJO IPSEC: permiso ip 192.168.30.0/255.255.255.0 192.168.20.0/
255.255.255.0
        SA Activas: 2, origen: mapa criptográfico
        Entrante:  #pkts dec'ed 335 drop 0 life (KB/Sec) 4429573/683
        Saliente: #pkts enc'ed 335 drop 0 life (KB/Sec) 4429573/683
--> FLUJO IPSEC: permiso ip 192.168.75.0/255.255.255.0 192.168.20.0/
255.255.255.0
        SA Activas: 0, origen: mapa criptográfico
        Entrante:  #pkts dec'ed 0 drop 0 life (KB/Sec) 0/0
        Saliente: #pkts enc'ed 0 drop 0 life (KB/Sec) 0/0

Interfaz: Serie 1/0:1
Estado de la sesión: ACTIVA, SIN IKE
Par: Puerto 10.130.1.2 500 fvrf: (ninguno) ivrf: (ninguno)
      Desc: (ninguno)
      Phase1_id: (ninguno)
--> FLUJO IPSEC: permiso ip 192.168.75.0/255.255.255.0 192.168.10.0/
255.255.255.0
        SA Activas: 0, origen: mapa criptográfico
        Entrante:  #pkts dec'ed 0 drop 0 life (KB/Sec) 0/0
        Saliente: #pkts enc'ed 0 drop 1 life (KB/Sec) 0/0
--> FLUJO IPSEC: permiso ip 192.168.30.0/255.255.255.0 192.168.10.0/
255.255.255.0
        SA Activas: 2, origen: mapa criptográfico
        Entrante:  #pkts dec'ed 725 drop 0 life (KB/Sec) 4492717/470
        Saliente: #pkts enc'ed 707 drop 1 life (KB/Sec) 4492717/470
. . .
```

Funciones de voz admitidas en múltiples sitios

Esta tabla indica las funciones de voz comunes e indica cuáles se admiten entre los sitios en una configuración de múltiples sitios.

Función de voz	Admitida entre múltiples sitios
Llamadas básicas de sitio a sitio con discado abreviado	Sí
Transferir llamadas entre sitios	Sí
Fono conferencias entre sitios	Sí
Localización y Parqueo de llamadas en los sitios	No
Envío de correos de voz entre sitios	No
Contestadora automática	Parcial La Contestadora automática puede transferir llamadas a otros anexos utilizando el discado abreviado del sitio.
Fax entre sitios	Sí
Movilidad de anexos entre sitios	No
Grupos de llamado configurados entre sitios	No
Directorio compartido entre sitios	No

Máximo de llamadas (Control de admisión de llamadas)

Para acceder a la configuración de control de admisión de llamadas, seleccione **Configurar** > **Telefonía** > **Administración del sitio** > **Máximo de llamadas** .

Visión general

El Control de admisión de llamadas (CAC) limita el número de llamadas simultáneas sobre la WAN. Cuando se activa y configura Control de admisión de llamadas, se aplica a todas las llamadas que pasan por la WAN. Ello incluye las llamadas entre sitios en una implementación de múltiples sitios y llamadas SIP.

Realice la configuración de Morfología de tráfico/QoS antes de configurar el Máximo de llamadas para que Configuration Assistant pueda determinar la configuración recomendada para CAC basada en estos valores.

Cuando se cambie esta configuración, el valor de **Número máximo de llamadas** configurado en la ventana Enlace SIP también se actualiza (**Configurar** > **Telefonía** > **Puertos y Enlaces** > **Enlaces SIP)**. Consulte **Troncal SIP, página 322**.

Procedimientos

Para configurar Control de admisión de llamadas, siga estos pasos:

PASO 1 Seleccione **Configurar** > **Telefonía** > **Administración del sitio** > **Máximo de llamadas** en la barra de funciones para abrir la ventana Máximo de llamadas.

PASO 2 Seleccione un dispositivo del campo Nombre de host.

PASO 3 En el campo Máximo de llamadas, especifique el número máximo de llamadas simultáneas que se permitirán.

Si se especifica un valor de cero (0), se activa el control de admisión de llamadas.

Si se activa y configura QoS para el sitio:

- La sección **Morfología de tráfico actual** muestra información de sólo lectura acerca de la configuración de Morfología del tráfico configurada actualmente en el sistema (ancho de banda de subida en Kbps y porcentaje de ancho de banda de WAN garantizado para las llamadas por VoIP).
- La sección **Intervalos máximos de llamadas** muestra los intervalos Recomendados, Sensibles y Degradados para la configuración de Máximo de llamadas basada en la configuración actual de QoS.

Si no se configura QoS, seleccione **Configurar** >**Enrutamiento**> **Conexión a Internet** en la barra de funciones, seleccione la conexión WAN, haga clic en **Modificar**, y seleccione la ficha Morfología de tráfico.

PRECAUCIÓN Si selecciona un nombre en el intervalo Sensible o Degradado para la configuración de Máximo de llamadas, esto puede ocasionar una mala calidad de voz para todas las llamadas de VoIP, incluyendo las llamadas entres sitios) si se supera el ancho de banda disponible.

PASO 4 Especifique el número máximo de llamadas que se permitirán para este sitio.

PASO 5 Haga clic en **Aceptar**.

17

Aplicaciones

Configuration Assistant entrega soporte para activar y configurar las aplicaciones de Cisco SBCS Smart y otras aplicaciones de terceros para las plataformas UC500.

Para algunas aplicaciones, deben determinarse opciones de configuraciones específicas para la aplicación para activarla y poder utilizarla.

Estos temas entregan información sobre la activación y configuración para las aplicaciones de Cisco SBCS:

- **Configuración general**
- **Administrador de Smart Applications**
- **Configuración específica para la aplicación**

Para obtener mayor información sobre las aplicaciones de terceros para Cisco SBCS, vaya a esta dirección en la Comunidad de soporte para pequeñas empresas de Cisco:

https://supportforums.cisco.com/docs/DOC-9780/

Configuración general

Algunas aplicaciones, como PhoneConnect de WebEx de Cisco u otras aplicaciones de terceros para SBCS, necesitan que se configuren los parámetros generales del sistema para que puedan funcionar. Para acceder a las configuraciones generales para las aplicaciones, seleccione **Aplicaciones** > **General Configuración** en la barra de funciones.

Las configuraciones generales que pueden configurarse se describen estas secciones:

- **URL de autenticación**
- **Acceso al menú de servicios**

- **Cuentas de llamadas**
- **Autenticación HTTPS**

Para obtener información detallada sobre las configuraciones generales para las aplicaciones, consulte la documentación de la aplicación que está configurando.

URL de autenticación

Esta ventana aparece cuando se selecciona **Aplicaciones** > **Configuración general** > **URL de autenticación** en la barra de funciones.

Esta configuración especifica la URL de autenticación CME necesaria para una aplicación Cisco SBCS Smart o una aplicación de terceros.

A continuación se encuentran algunos ejemplos de URL de autenticación:

- VoiceView Express

  http://10.1.10.1/voiceview/authentication/authenticate.do

- PhoneConnect de WebEx

  http://10.1.10.2/CCMCIP/authenticate.asp.

Sólo puede utilizarse una URL de autenticación a la vez. Para configurar una aplicación y URL de autenticación diferente, primero se debe desactivar la aplicación que esté utilizando dicha configuración. Por ejemplo, se debe desactivar PhoneConnect de WebEx si se necesita configurar una URL de autenticación para integrarla con una aplicación de terceros.

NOTA Algunas URL de autenticación son compatibles con más de una aplicación para Cisco SBCS. Por ejemplo, la URL de autenticación para VoiceView Express también es compatible con la URL de autenticación para TimeCardView. La URL de la aplicación PhoneConnect de WebEx es compatible tanto con VoiceView Express como con TimeCardView, y estas aplicaciones puede activarse simultáneamente si hay suficientes recursos para ejecutarlas.

Cuando se accede por primera vez a la ventana URL de autenticaicón, se muestra la URL de autenticación para VoiceView Express. Esto se debe a que la configuración por defecto para VoiceView Express es **Activado**. Configuration Assistant configura autómáticamente la URL de autenticación para la aplicación y la URL de servicio CME para VoiceView Express cuando se inicia el sistema de voz. Para activar o desactivar VoiceView Express, seleccione **Configurar** > **Telefonía** > **Usuarios y anexos** > **Correo de voz**, y seleccione la ficha Configuración.

No todas las aplicaciones requieren una URL de autenticación. Consulte la documentación de la aplicación que está configurando para determinar la URL que especificará aquí. Algunas aplicaciones configuran esta URL automáticamente cuando se activan.

Haga clic en **Aceptar** o en **Aplicar** cuando haya especificado la URL de autenticación.

Acceso al menú de servicios

Esta ventana aparece cuando se selecciona **Aplicaciones** > **Configuración general** > **Acceso al menú de servicios** en la barra de funciones.

- **Visión general**
- **Agregar una URL de Servicios CME**
- **Modificar o Eliminar una URL de Servicios CME**

Visión general

En la ventana Acceso al menú de servicios, se define el nombre del elemento del menú, la URL del servicio CME y el orden de los elementos del menú en los teléfonos IP para las URL de servicio configurables. Las utilizan aplicaciones como PhoneConnect de WebEx, TimeCardView y otras aplicaciones de terceros. Los elementos del menú que se definen aquí se muestran cuando el usuario presiona el botón **servicios** en su teléfono IP.

Pueden configurarse hasta 8 URL de servicios.

Utilice los botones con las flechas **Hacia arriba** y **Hacia abajo** para cambiar el orden en que se muestran en el menú de **servicios** en los teléfonos IP.

Sólo puede modificarse el orden de las URL de servicios CME configurables. En el menú de **servicios** del teléfono IP de Cisco, el elemento de la URL del servicio CME siempre aparece primero, seguido de los elementos de las URLS del servicio CME configurables, de Movilidad de anexo y de Apps de mi teléfono.

IMPORTANTE Consulte la documentación de la aplicación que está configurando para la URL especifica que se indicará.

- Algunas aplicaciones, como PhoneConnect de WebEx y VoiceView Express configuran automática esta URL por usted.
- Si una aplicación configura automáticamente una URL de servicios cuando se activa, la URL de servicios se elimina de inmediato de la lista cuando se

desactiva la aplicación. No se puede modificar ni eliminar las URL de servicios que estas aplicaciones hayan configurado.

Agregar una URL de Servicios CME

Para agregar una nueva URL de servicios CEM, siga estos pasos:

PASO 1 Haga clic en **Agregar** para abrir una nueva una fila en la tabla para su edición.

PASO 2 Configure el nombre y URL del servicio.

Configuración	Descripción
Nombre del menú	El nombre del menú de servicios CME que aparecerá en el menú Servicios de los teléfonos IP de Cisco. El nombre del menú puede tener hasta 15 carácteres y no debe incluir espacios ni catácteres especiales.
URL	La URL de servicios CME, por ejemplo: http://10.1.10.1/WebExPhone/MainMenu

PASO 3 Si se indican múltiples URL de servicios CME, utilice los botones de flechas **Hacia arriba** y **Hacia abajo** para organizar el orden de los elementos del menú.

PASO 4 Haga clic en **Aceptar**.

Modificar o Eliminar una URL de Servicios CME

No se puede modificar ni eliminar las URL de servicios por defecto que configuran automáticamente las aplicaciones SBCS, tales como VoiceVew Express, TimeCardView o WebEx PhoneConnect. Sin embargo, se puede desactivar estas aplicaciones para quitar las URL de servicios.

Las URL de servicios configuradas por el usuario pueden eliminarse o modificarse según sea necesario.

- Para modificar una URL de servicios configurada por el usuario, haga clic en la columna Nombre del menú o URL para la fila que contenga la URL, realice la edición y haga clic en **Aceptar** o en **Aplicar**.
- Para eliminar una URL de servivios configurada por el usuario, seleccione la URL de la lista y haga clic en **Eliminar**.

Cuentas de llamadas

La ventana Cuentas de llamadas aparece cuando se selecciona **Aplicaciones** > **Configuración general** > **Cuenta de llamadas** en la barra de funciones.

Visión general

En esta ventana, se puede activar o desactivar la recolección de CDR (Registro de detalles de llamadas) y especificar la ubicación de un servidor TFTP op FTP externo donde se almacenen los CDR, así como también una ubicación de copia de seguridad en la memoria flash UC500. Esta configuración se utilizan en conjunto con las aplicaciones de cuenta de llamadas que capturan los CDR y los almacenan en un servidor FTP externo.

Los archivos de copia de seguridad CDR se guardan en el directorio flash:crd/ del UC500. Haga clic en **Copiar CDR a archivo** para guardar manualmente los CDR en el archivo de seguridad especificado en la memoria flash.

Para obtener mayor información, consulte la documentación de la aplicación de cuenta de llamadas que está configurando.

Procedimientos

Configure la configuración general para todas las aplicaciones de Cuenta de llamadas como se describe en esta tabla. Haga clic en **Aceptar** o en **Aplicar** cuando haya finalizado.

Configuración	Descripción
Servidor de cuenta de llamadas	
URL de FTP	Configura la ubicación primaria para almacenar los CDR generados para el control de archivos. Especifique una ruta/nombre de archivo para la ubicación del archivo en un servidor FTP. Por ejemplo: ftpserver01/cdrs
Nombre de usuario	El nombre de usuario para la autenticación en el servidor FTP.
Contraseña	La contraseña para la autenticación en el servidor FTP.

Configuración	Descripción
Copia de seguridad de la memoria flash	
Nombre del archivo de seguridad de la memoria flash	El nombre de archivo base que se utiliza para las copias de seguridad de los CDR en el directorio flash:\cdr\ del UC500, por ejemplo, `cdr_backups`. El nombre del archivo puede tener hasta 15 caracteres alfanuméricos. No se admiten espacios ni carácteres especiales. El archivo de seguridad de CDR recibe un nombre único cuando se crea. El nombre de host del router y la hora se agregan al nombre del archivo en formato *<nombre de archivo>.<nombre de host>.<hora>*. Por ejemplo, si el **Nombre de archivo de seguridad de la memoria flash** es `cdr_backups`, la ruta y el nombre del archivo se formatean como se indica a continuación: `flash:/cdr/ cdr_backups.UC520.07_25_2009_18_15_10.346`
Copiar CDR a archivo	Haga clic en **Copiar CDR a archivo** para copiar manualmente la información de CDR pendiente al archivo de seguridad de CDR en la memoria flash UC500. Cuando se hace clic en **Copiar CDR a archivo**, se crea un nuevo archivo CDR de seguridad en la memoria flash.

Autenticación HTTPS

Esta ventana aparece cuando se selecciona **Aplicaciones** > **Configuración general** > **Autenticación HTTPS** en la barra de funciones.

Algunas aplicaciones, como PhoneConnect de Cisco WebEx, requieren que se active la comunicación HTTPS y se indique un nombre de usuario y contraseña para la autenticación.

Para obtener información adicional, consulte la documentación de la aplicación que se está configurando.

Configure la **Autenticación HTTPS** como se describe en esta tabla. Haga clic en **Aceptar** o en **Aplicar** cuando haya finalizado.

Configuración	Descripción
Activar comunicación HTTPS	Cuando está activada (marcada), esta configuración crea el certificado HTTPS privado que se utiliza para conectarse al API de servicios web de PhoneConnect. Esta opción debe estar marcada para PhoneConnect de WebEx.
Nombre	Nombre de usuario para la autenticación HTTPS. El nombre de usuario puede tener hasta 15 caracteres. No se admiten espacios ni carácteres especiales. Por defecto, este campo está vacío. Es necesario para PhoneConnect de WebEx.
Contraseña	La contraseña para la autenticación HTTPS. La contraseña puede tener hasta 15 caracteres. No se admiten espacios ni carácteres especiales. Por defecto, este campo está vacío. Es necesario para PhoneConnect de WebEx.

Administrador de Smart Applications

Para acceder a opciones para activar y desactivar Smart Applications, seleccione **Aplicaciones** > **Administrador de Smart Applications** en la barra de funciones.

Visión general

En el Administrador de Smart Applications, se puede activar, desactivar y configurar Smart Aplications de Cisco SBCS. Estas aplicaciones se ejecutan en el módulo CUE de la plataforma UC500. También se puede visualizar el total de recursos disponible, los recursos requeridos para cada aplicación y la utilización actual de cada aplicación. Las aplicaciones que se pueden activar en esta ventana incluyen:

- Mensajería unificada
- PhoneConnect de WebEx de Cisco
- TimeCardView de Cisco

Los recursos del sistema que una aplicación utiliza se indican mostrando el número de créditos. Está disponible un total de 100 créditos para el sistema. El número de créditos requerido para cada aplicación es la cantidad de créditos mínimia necesaria para ejecutar la aplicación, basada en la utilización de CPU, memoria y disco. Algunas aplicaciones, como Video Telefonía y Grabación en vivo no requieren créditos para ejecutarse. Configuration Assistant indica un error si se intenta activar una aplicación sin la cantidad de recursos requeridos.

Para activar o desactivar una aplicación:

PASO 1 En la lista Aplicaciones de la izquierda, haga clic en la aplicación que desea activar.

Se muestra una breve descripción de la aplicación,

PASO 2 Haga clic en **Configurar** para acceder a las opciones para activar y configurar la aplicación.

Consulte estas secciones para tener mayor información sobre la configuración de Cisco SBCS Smart Applications:

- **Mensajería unificada (IMAP), página 529**
- **PhoneConnect de WebEx de Cisco, página 530**
- **TimeCardView, página 544**.

PASO 3 Haga clic en **Aceptar** o en **Aplicar** cuando haya finalizado de configurar la aplicación.

Configuración específica para la aplicación

Los temas de esta sección entregan una visión general de cada aplicación junto con instrucciones para configurar las opciones de configuración específicas para la aplicación.

- **Mensajería unificada (IMAP)**
- **Vídeo Telefonía**
- **PhoneConnect de WebEx de Cisco**
- **TimeCardView**

Mensajería unificada (IMAP)

Aparece la ventana Configuración de mensajería unificada cuando se selecciona Mensajería unificada en la lista Aplicaciones de la ventana Administrador de Smart Applications y se hace clic en **Configurar**.

Visión general

La Mensajería unificada permite que los suscriptores de correo de voz tengan una visión integrada de sus mensajes de correo electrónico y de correo de voz desde un solo cliente de correo electrónico utilizando IMAP. Los suscriptores puede eliminar mensajes del correo de voz o marcarlos como leídos o no leídos de la misma manera que los mensajes de correo electrónico. Los mensajes de correo de voz se descargan como adjuntos a los mensajes de correo de voz. Los suscriptores pueden acceder a los mensajes de correo de voz a través de la red o descargarlos en forma selectiva. La configuración por defecto para esta aplicación es desactivada.

Procedimientos

Activar o desactivar Mensajería unificada

Para activar o desactivar Mensajería unificada, haga clic en la casilla **Activar mensajería unificada** y luego, en **Aceptar** para volver a la ventana del Administrador de Smart Applications.

Configuración del cliente de IMAP

Para que un usuario aproveche esta función, su cliente de correo electrónico (por ejemplo, Microsoft Outlook) debe estar configurado para IMAP. Al configurar el cliente para IMAP:

- Utilice la dirección IP (10.1.10.1) del módulo de Cisco Unity Express (CUE) para la dirección IP del servidor IMAP.
- El nombre de usuario y contraseña configurados en el cliente IMAP para la autenticación deben coincidir con el nombre de usuario y contraseña del usuario telefónico tal como están configurados en Cisco Configuration Assistant.

Vídeo Telefonía

La solución Cisco Unified Video Advantage (CUVA) de SBCS permite que los usuarios realicen llamadas de vídeo telefonía de escritorio a escritorio entre los teléfonos IP de Cisco IP que tengan capacidad de vídeo.

La Vídeo telefonía está activada por defecto. Para desactivar esto, desmarque la opción **Activar vídeo telefonía** y haga clic en **Aceptar**.

Puede seleccionar si se permiten las llamadas con vídeo en teléfonos específicos activando o desactivando la opción **Permitir llamadas con vídeo** en cada teléfono. Consulte **Permitir llamadas de vídeo, página 332**.

PhoneConnect de WebEx de Cisco

PhoneConnect de WebEx está diseñado para clientes que desean un acceso rápido y simple a las reuniones WebEx desde sus teléfonos IP sin la necesidad de una PC de escritorio. PhoneConnect de WebEx automatiza todo este proceso para que los usuarios de teléfonos IP puedan conectarse al audio de una conferencia de WebEx presionando una sola tecla de su teléfono IP. Esta sección cubre los siguientes temas:

- **Acerca de PhoneConnect de WebEx de Cisco**
- **Requerimientos de la plataforma SBCS**
- **Documentación relacionada**
- **Información de cuenta del administrador del sitio de WebEx**
- **Procedimientos**

Acerca de PhoneConnect de WebEx de Cisco

Una vez que un usuario de WebEx se asocia a un teléfono IP por medio de PhoneConnect de WebEx, una simple aplicación de navegador de reuniones se instala en la pantalla de su teléfono IP que permite que el usuario del teléfono IP:

- Escuche las reuniones de WebEx a la que están invitando
- Escuche las reuniones de WebEx a las que son invitados por otros usuarios de teléfonos IP de su empresa (los usuarios deben compartir el mismo router UC500)
- Reciban alertas visuales y auditivas en su teléfono IP cuando sea hora de participar en una reunión
- Controlen con cuánta anticipación de la reunión desean recibir las alertas
- Presionen una sola tecla para participar de una reunión

Los usuarios de WebEx con acceso a un cliente de WebEx Connect desde una PC de escritorio pueden usar la función Hacer clic para llamar con su teléfono IP para llamar automáticamente a alguien en su Lista de contactos de WebEx Connect.

Requerimientos de la plataforma SBCS

Componente	Versión
Cisco Configuration Assistant (CCA)	2.0 y posterior
Paquete de software de UC500	7.0(3) ó posterior
IOS de Cisco	12.4(20)T2 ó posterior Cisco Unified Communications Manager Express (CME) 7.0 ó posterior
Cisco Unity Express (CUE)	CUE 7.0 ó posterior
Teléfonos IP de Cisco admitidos	Teléfonos IP unificados de Cisco, modelos 794x, 796x y 797x Teléfonos inalámbricos unificados de Cisco modelos 7921 y 7925 Teléfono IP unificado de Cisco modelo 7937 Teléfono IP unificado de Cisco modelo 524G Teléfono IP unificado de Cisco modelo 521G Teléfonos IP SPA525G y SPA525G2 de Cisco Cliente de softphone de Comunicador IP de Cisco (CIPC)

Documentación relacionada

Para obtener información detallada sobre la configuración y administración de PhoneConnect de WebEx, consulte la *Guía de administración de PhoneConnect de WebEx de Cisco*.

La información e instrucciones para el usuario final se documentan en la *Guía de referencia rápida de PhoneConnect de WebEx de Cisco*.

Información de cuenta del administrador del sitio de WebEx

Antes de poder activar y configurar la aplicación PhoneConnect de WebEx, su cliente debe tener u obtener una cuenta WebEx de pequeña empresa con un usuario administrativo.

- Su cliente debe entregarle la información de la cuenta del sitio de servicios WebEx (una ID y contraseña de usuario administrativo, la ID del usuario y la URL del sitio).

  CCA utiliza esta información para conectarse a las instalaciones del cliente de servicios de WebEx WebEx y asociar cuentas de usuario del cliente con la aplicación WebEx PhoneConnect.

- Asegúrese que usted conoce la política de contraseñas utilizadas para el sitio.

  Cuando se configura un sitio WebEx, el administrador del sitio puede especificar una política de contraseñas. La política define los requerimientos de contraseñas de usuarios, como el número mínimo y máximo de carácteres, seguridad de contraseña, los carácteres que no pueden estar en las contraseñas, etc. Todas las contraseñas de usuarios de WebEx deben ajustarse a esta política.

Antes de comenzar

Antes de configurar PhoneConnect de WebEx, asegúrese que:

- Los anexos de teléfonos y usuarios estén configurados en el sistema (**Configurar** > **Telefonía** > **Usuarios y anexos> Usuarios y teléfonos** > ficha **Anexos de usuarios**).
- Se haya configurado el plan de numeración y los troncales de voz y que las llamadas entrantes y salientes estén funcionando correctamente.
- Esté configurada la dirección IP del servidor DNS. PhoneConnect de WebEx utilice la dirección IP del servidor DNS del Proveedor de servicio de Internet para ubicar al servidor webex.com.
- Esté configurado el servidor NTP (opcional; recomendado para la sincronización de las horas y alertas de reuniones).

Procedimientos

Lea esta sección para tener una visión general de los pasos de configuración de PhoneConnect de WebEx. Para obtener información más detallada, consulte la *Guía de administración de PhoneConnect de WebEx de Cisco*, disponible en Cisco.com.

Para configurar PhoneConnect de WebEx de Cisco, siga estos pasos:

PASO 1 Inicie Cisco Configuration Assistant y conéctese al UC500 de Cisco.

PASO 2 Seleccione **Aplicaciones > Configuración general > URL de Autenticación** en la barra de funciones. En la ventana URL de autenticación, configure estos parámetros:

a. Verifique que se está utilizando `http://10.1.10.2/CCMCIP/authenticate.asp` para la URL. Si no, modifique la configuración para que lo esté.

b. Haga clic en **Aceptar**.

PASO 3 Seleccione **Aplicaciones** > **Configuración general** > **Autenticación HTTPS** en la barra de funciones.

PASO 4 En la ventana Autenticación HTTPS, configure estos parámetros:

a. Marque **Activar Comunicación HTTPS** (requerido).

b. Especifique un nombre de usuario y contraseña para la autenticación HTTPS (requerido).

c. Haga clic en **Aceptar**.

Los parámetros de la URL de servicios CME para PhoneConnect de WebEx se completan automáticamente después que se active la aplicación PhoneConnect.

PASO 5 Navegue hasta **Aplicaciones** > **Administrador de Smart Applications**.

PASO 6 Haga clic en **Phone Connect de WebEx** para seleccionar la aplicación y, luego, haga clic en la casilla **Configurar**. Aparece la ventana de Inicio de Sesión de Configuración de PhoneConnect.

PASO 7 En la ventana Inicio de sesión de configuración de Phone Connect, especifique el nombre de usuario y contraseña del administrador de WebEx y también la ID y URL del sitio y haga clic en **Aceptar**. Consulte **Ventana Inicio de sesión de configuración de Phone Connect, página 534**.

Una vez que se verifican las credenciales de inicio de sesión, aparece la ventana principal de Aplicaciones de PhoneConnect y muestra información para el sitio WebEx.

PASO 8 En la ventana principal de Aplicaciones de PhoneConnect, haga clic en la casilla **Activar** de la parte superior de la ventana y configure el sitio. Consulte **Ventana Aplicación principal de PhoneConnect, página 535**.

PASO 9 Agregue los usuarios y active PhoneConnect de WebEx en sus teléfonos IP de Cisco como se describe en la *Guía de administración de PhoneConnect de WebEx* de Cisco. Consulte **Ventana Aplicación principal de PhoneConnect, página 535**.

PASO 10 Haga clic en **Aceptar** para aplicar la configuración del sitio y cerrar la ventana Aplicación principal de PhoneConnect.

PASO 11 En la ventana del Administrador de Smart Applications, haga clic en **Aceptar**.

Consulte **Configuración avanzada del sitio de PhoneConnect, página 541** para obtener información sobre configuraciones adicionales que sea necesario realizar.

Ventana Inicio de sesión de configuración de Phone Connect

Para configurar PhoneConnect, primero se debe iniciar sesión con las credenciales de la cuenta del administrador del sitio WebEx, como se describe a continuación.

Configuración	Descripción
ID de usuario	ID de usuario administrador del sitio WebEx. También se le conoce como ID WebEx.
Contraseña	Contraseña del administrador del sitio WebEx
ID del sitio	Número de la ID del sitio WebEx (no se aceptan carácteres de texto en este campo).
Nombre del sitio	Nombre del sitio WebEx (la primera cadena de la URL del sitio WebEx). Por ejemplo, si la URL del sitio WebEx es http://acme.webex.com, especifique acme para el nombre del sitio.

Haga clic en **Aceptar** cuando haya finalizado de especificar las credenciales de inicio de sesión.

Ventana Aplicación principal de PhoneConnect

Esta ventana aparece cuando se ha iniciado con éxito la sesión con las credenciales del administrador del sitio WebEx después de hacer clic en **Opciones de configuración** para PhoneConnect de WebEx en la ventana del Administrador de Smart Applications.

Defina la configuración en la Ventana principal de la aplicación PhoneConnect como se describe a continuación. Haga clic en **Aceptar** o en **Aplicar** cuando haya finalizado de hacer cambios.

Configuración	Descripción
Información del administrador de clientes Información de contacto del administrador del sitio WebEx.	
Nombre	Nombre del administrador del sitio WebEx
Apellido	Apellido del administrador del sitio WebEx
Correo electrónico	Dirección de correo electrónico del administrador del sitio WebEx
Empresa	Nombre de la empresa del administrador del sitio WebEx
Teléfono	Número de teléfono del administrador del sitio WebEx

Configuración	Descripción
Información de usuarios de WebEx	
ID de usuario	Requerido. Esta es la ID del usuario de la cuenta WebEx que el usuario especifica cuando se inicia la sesión en el sitio de servicios WebEx para calendarizar, asistir y explorar las reuniones. Formato recomendado: *<ID del usuario telefónico>*@*<dominio del administrador>*.com Todos los nuevos usuarios de WebEx creados a través de PhoneConnect deben utilizar el formato de dirección de correo para su ID de usuario. Las cuentas de usuario de WebEx creadas antes de que se activara PhoneConnect pueden seguir utilizando el formato de ID de usuario existente. Si todos los usuarios de sus clientes comparten el mismo dominio de correo electrónico, se recomienda que agregue dominio de correo electrónico de su cliente después de que el ID de usuario del teléfono, y utilizar esto como el identificador de usuario, por ejemplo, jsmith@acme.com.
Contraseña	Requerido. Esta es la contraseña que el usuario especifica cuando inicia sesión en el sitio de servicios WebEx para invitar, asistir o explorar reuniones. Cuando se configura un sitio WebEx, el administrador del sitio puede especificar una política de contraseñas. La política define criterios para las contraseñas de usuarios, como número de carácteres, las contraseñas que no pueden utilizarse, etc. Todas las contraseñas de usuario deben ajustarse a la directiva de contraseñas para el sitio de su cliente de servicios de WebEx. Asegúrese de notificar a los usuarios si se les cambia la contraseña.

Configuración	Descripción
Correo electrónico	Requerido. Esta es la dirección de correo electrónico a la que se envían las invitaciones a reuniones y avisos WebEx. Si el usuario no tiene una dirección de correo electrónico (por ejemplo, el usuario es una sala de reuniones, se recomienda el siguiente formato: <*ID del usuario telefónico*>@<*dominio del administrador*>.com donde la <*ID del usuario telefónico*> es la ID asociada al campo Usuario telefónico asociado.
Apellido	Requerido. Nombre del usuario de la cuenta WebEx.
Nombre	Requerido. Apellido del usuario de la cuenta WebEx.
Teléfono asociado	Sólo lectura. Muestra la ID del usuario telefónico actual asociada a esta cuenta WebEx. Si no hay una ID de usuario telefónico asociada al usuario de PhoneConnect de WebEx, se muestra --Ninguno--.
Seleccionar teléfono	Haga clic en **Seleccionar teléfono** para abrir un diálogo y seleccionar un usuario telefónico asociado a esta cuenta de usuario de WebEx y activar la aplicación PhoneConnect en su teléfono. Consulte **Seleccionar teléfono, página 540**. Si el usuario tiene una cuenta WebEx existente y tiene un teléfono configurado en el sistema, pero no tiene un PhoneConnect activado en su teléfono, se puede utilizar Seleccionar teléfono para activar la aplicación PhoneConnect en su teléfono. **IMPORTANTE**: Si está editando una cuenta de usuario de WebEx existente para activar PhoneConnect, debe asignarle al usuario de WebEx una nueva contraseña (esto es necesario para que PhoneConnect pueda autenticar al usuario telefónico). Asegúrese de notificar al usuario de su nueva contraseña de cuenta WebEx.
Agregar	Insertar una nueva fila en la lista de usuarios de WebEx para agregar a un nuevo usuario.

Configuración	Descripción
Eliminar	Elimine el usuario de WebEx seleccionado. El usuario pasa a un estado desactivado en el sitio de servicios WebEx. Una vez que se elimina una cuenta de usuario, éste ya no tiene acceso a WebEx ni a PhoneConnect de WebEx. El usuario ya no recibirán las invitaciones a reuniones o alerta, y no podrá asistir o sede de las reuniones de WebEx desde el sitio de su compañía de servicios de WebEx. Para volver a instaurar a un usuario después que haya sido eliminado (por ejemplo, si un usuario abandona la empresa, pero luego, retorna), se puede utilizar su antigua ID de usuario y la restante información de la cuenta. Sin embargo, debe crearse una nueva contraseña, ya que WebEx puede configurarse para que rechace una contraseña que sea igual a cualquiera de las últimas tres contraseñas registradas previamente en WebEx.
Copiar desde dispositivo	**Copiar desde dispositivo** es un método alternativo para agregar usuarios de WebEx. Haga clic en **Copiar desde dispositivo** para abrir un diálogo y seleccionar los usuarios telefónicos existentes que se van a asociar a esta cuenta WebEx. El nombre, apellido, contraseña y teléfono para cada usuario seleccionado se copian en la lista de usuarios de WebEx. Los campos ID de usuario de WebEx y Dirección de correo electrónico se dejan en blanco. Consulte **Copiar desde dispositivo, página 540**.
Información de configuración del sitio del cliente	
Instalar archivos de idiomas	Añadir un nuevo lenguaje adaptado a los usuarios de WebEx teléfono IP "PhoneConnect navegador de reuniones y alertas. Sólo las pantallas de los teléfonos IP de PhoneConnect de WebEx se ven afectadas por este procedimiento. Consulte **Instalar archivo de idioma para PhoneConnect de WebEx, página 543**.

Configuración	Descripción
Configuración avanzada	Configuración avanzada de acceso. Consulte **Configuración avanzada del sitio de PhoneConnect, página 541**.
Configuración de llamada de reunión	
Preferencia de llamadas	Utilice un número de teléfono sin cargo o con cargo para la llamada de reuniones de WebEx. Por defecto, es sin cargo.
Prefijo de discado	Dígito que quien llama disca para obtener una línea saliente. El valor por defecto es el código de acceso para el discado externo definido en el sistema. Puede editar esta configuración.
Conversión de números de llamada - Número con cargo o sin cargo Despendiendo desde dónde está llamando su cliente, cómo esté configurado su plan de numeración saliente y cómo esté formateado el número de llamada de WebEx, se podría necesitar utilizar esta configuración para quitar o reemplazar los prefijos de discado inicial, como códigos de país, códigos de área o ciudad o códigos para discado internacional.	
Número entregado por WebEx	Sólo lectura. Número de teléfono entregado por WebEx para este sitio.
Quitar número de dígitos del frente	Número de dígitos que se van a quitar desde el inicio del número entregado por WebEx. Este campo es obligatorio y no puede dejarse vacío. El valor, por defecto, es cero (0). Especifique el número de dígitos que debe quitarse o reemplazarse según sea necesario para coincidir con el número de discado saliente.
Agregue dígitos al frente	Dígitos que se agregan al comienzo del número de llamada entregado por WebEx. Este campo puede tener hasta 20 dígitos. El valor por defecto es Ningungo (vacío). Especifique los dígitos que se van a agregar al frente del número, por ejemplo, un código de área que sea distinto al que entrega WebEx. No se necesita agregar el Prefijo de discado saliente (código de acceso) aquí. El Prefijo de discado saliente se agrega en forma automática al frente del número.

Configuración	Descripción
Números resultantes de dígitos que se deben discar	Número de discado saliente después de agregar y quitar dígitos y dejando pendiente el prefijo de discado saliente. El número indicado es de sólo lectura y se genera utilizando el Prefijo de discado saliente y los valores especificados en los campos Prefijo de discado saliente y Quitar/Agregar dígitos. Verifique que el número coincida con lo que los usuarios discan manualmente para obtener el servicio WebEx.

Seleccionar teléfono

Esta ventana aparece cuando se hace clic en **Seleccionar teléfono** en la lista de usuarios de WebEx en la ventana Aplicación principal de PhoneConnect de WebEx de Cisco.

PASO 1 En la ventana Seleccionar teléfono, seleccione uno de la lista que desee asociar con este usuario de PhoneConnect de WebEx.

Sólo se indican los teléfonos que no estén activados actualmente para PhoneConnect.

PASO 2 Haga clic en **Aceptar** para volver a la ventana Aplicación principal de PhoneConnect de WebEx.

Copiar desde dispositivo

Esta ventana aparece cuando se hace clic en **Copiar desde dispositivo** en la ventana Aplicación principal de PhoneConnect de WebEx.

La opción **Copiar desde dispositivo** entrega una forma conveniente para agregar cuentras de WebEx y activar PhoneConnect para múltiples usuario de teléfonos existentes. Cuando se utiliza **Copiar desde dispositivo**, los valores provisionados previamente se copian en forma automática en los campos adecuados de la cuenta del usuario de WebEx.

Para utilizar **Copiar desde dispositivo**, siga estos steps:

PASO 1 Seleccione uno o más usuarios telefónicos para los que desee agregar cuentas de WebEx. Sólo se indican los teléfonos que no estén asociados a una cuenta de usuario de WebEx.

PASO 2 Haga clic en **Seleccionar todo**o utilice los accesos directos del teclado CTRL-clic y SHIFT-clic para seleccionar múltiples usuarios.

PASO 3 Haga clic en **Agregar** para transferir usuarios telefónicos a la lista de usuarios seleccionados.

PASO 4 Haga clic en **Aceptar**.

La ID del usuario, su nombre y apellido, dirección de correo electrónico y teléfono asociado con cada usario telefónico existente se copian en la lista de usuarios de WebEx de la ventana Aplicación principal de PhoneConnect. La contraseña se deja en blanco.

PASO 5 En la ventana Aplicación principal de PhoneConnect se debe ubicar a los usuario que se acaban de agregar y completar el campo Contraseña.

Tan pronto como se asocie un teléfono IP con un usuario de WebEx, tendrá plena funcionalidad de PhoneConnect de WebEx. El teléfono IP no necesita ser reiniciado. Los menús abiertos en los teléfonos podría necesitar cerrarse para ver los cambios.

Configuración avanzada del sitio de PhoneConnect

Para acceder a la configuración avanzada para PhoneConnect de WebEx, haga clic en **Configuración avanzada del sitio** en la ventana Aplicación principal de PhoneConnect.

En la mayoría de los casos, se puede utilizar la configuración por defecto. Sólo se necesita hacer cambios si está experimentando problemas con PhoneConnect de WebEx.

Configure la configuración avanzada del sitio para la aplicación PhoneConnect de WebEx como se describe a continuación. Haga clic en **Aceptar** o en **Aplicar** cuando haya finalizado de configurar el sitio.

Configuración	Descripción
Configuración de la sincronización de la aplicación	

Configuración	Descripción
Buscar nuevas reuniones (minutos)	Frecuencia de encuesta en WebEx para nuevas reuniones. El valor, por defecto, es 4 minutos. Si se reduce la frecuencia a menos de 4 minutos se puede afectar negativamente el desempeño de Cisco Unity Express (CUE).
Retraso antes de entregar la ID de la reunión (segundos)	Número de segundos que el sistema espera después que se presiona el botón de llamada en el teléfono IP antes de especificar automáticamente la ID de la reunión. La configuración por defecto de 10 minutos se basa en la conectividad del enlace FXO/BRI/PRI. Este valor puede configurarse en 7 sesgundos si se utilizan enlaces SIP. Tal vez sea necesario aumentar el intervalo si se hacen llamadas internacionales. No hay impactos conocidos sobre el desempeño.
Retraso entre dígitos (milisegundos)	La velocidad con la que se discan los dígitos cuando se especifica automáticamente una ID de reunión. El valor por defecto es 200 ms. Tal vez sea necesario aumentar el intervalo, dependiendo de hacia dónde se hace la llamada (por ejemplo, cuando se hacen llamadas internacionales). No hay impactos conocidos sobre el desempeño.
Borrar datos del sitio de WebEx	Haga clic en **Borrar datos del sitio de WebEx** para eliminar todos los datos del sitio de WebEx del UC500. Esto no afecta la información de cuentas o sitio de servicios de WebEx; sólo elimina la configuración de la aplicación WebEx PhoneConnect y los datos del sitio guardados en el UC500 de Cisco. La aplicación PhoneConnect se elimina para todos los teléfonos de usuarios. Esto puede ser necesario, por ejemplo, en situaciones en que se importan datos equivocados al UC500, cambia el sitio de WebEx, éste ya no está activo o cuando los datos del sitio de demostración deben eliminarse del sistema.

Instalar archivo de idioma para PhoneConnect de WebEx

Para instalar un nuevo archivo de idioma localizado para PhoneConnect de WebEx, haga clic en **Instalar archivo de idioma** en la ventana Aplicación principal de PhoneConnect de WebEx de Cisco.

PhoneConnect de WebEx admite la localización de las pantallas GUI de los teléfonos IP para el navegador de reuniones de PhoneConnect de WebEx y para alertas. Entre versiones, Cisco agrega soporte para idiomas adicionales a medida que estén disponibles. Se puede actualizar la aplicación PhoneConnect de WebEx con un nuevo idioma utilizando la opción Instalar nuevo archivo de idiom. Una vez que esté instalado el nuevo archivo de idioma y éste se haya seleccionado en Configuration Assistant, todos los menús de las pantallas de los teléfonos IP de PhoneConnect de WebEx utilizarán este nuevo idioma.

Antes de comenzar, primero se debe localizar el UC500 a la región e idioma deseado (**Configurar** > **Telefonía** > **Sistema** >**Región**), luego descargue el correspondiente archivo de localización de WebEx para el nuevo idioma.

NOTA PhoneConnect de WebEx no admite la función de anulación de localización en el teléfono UC500. PhoneConnect de WebEx sólo muestra el idioma seleccionado por defecto.

Siga estos pasos para agregar un nuevo idioma para PhoneConnect de WebEx.

PASO 1 En el campo **Archivo a instalar**, navegue hasta el archivo de idioma que desea instalar y haga clic en **Abrir**.

PASO 2 Haga clic en **Instalar**. El nuevo archivo de idioma se transfiera a la lista de Archivos de idiomas instalados. Se puede sobreescribir un archivo de idioma existente, pero no se puede eliminarlo.

PASO 3 Haga clic en **Aceptar** para implementar el archivo de idioma en el directorio de localización CME y volver a la ventana Aplicación principal de PhoneConnect.

Se le pedirá reiniciar el módulo CUE en el UC500.

PASO 4 Para reiniciar el módulo CUE en el UC500, abra la vista Topología, haga clic con el botón derecho en el UC500 y seleccione **Reiniciar CUE** del menú.

El reinicio de CUE puede tomar de 10 a 15 minutos. Durante dicho lapso, estarán disponibles el correo de voz, la Contestadora automática y otras aplicaciones que necesiten una conexión a CUE.

TimeCardView

Esta ventana aparece cuando se selecciona TimeCardView en la lista Aplicaciones de la ventana del Administrador de Smart Applications y haga clic en **Configurar**.

IMPORTANTE Esta sección sólo cubre la configuración de TimeCardView y la del servidor de nóminas que pueden administrarse a través de Configuration Assistant. Para obtener mayor información, consulte la documentación indicada en **Documentación de TimeCardView, página 545**.

TimeCardView es un sistema de hora y asistencia para los usuarios de teléfonos IP de Cisco conectados a las plataformas SBCS de Cisco.

- **Visión general**
- **Documentación de TimeCardView**
- **Requerimientos de la plataforma SBCS**
- **Configuración de TimeCard**
- **Configuración del servidor de nóminas**

Visión general

TimeCardView automatically tracks employees' working hours and enables supervisors to view employees' real time status. Permite una revisión y aprobación en línea de las hojas de horarios y puede generar los informes que los supervisores y especialistas en nóminas necesita por medio del Cliente de informes históricos y exportarlos a los formatos .csv y .xls.

TimeCardView permite que los empleados utilicen un teléfono IP unificado de Cisco conectado a Unity Express de Cisco para dar seguimiento automáticamente a las horas trabajadas (inicio y término del turno, almuerzos y descansos) y revisar las horas por turnos, días, semanas y meses.

Los supervisores y especialistas en nóminas utilizan TimeCardView para configurar límites a las horas que los empleados pueden pasar en cualquier estado, ver su estado en el turno actual y aprobar sus hojas de horario.

Opcionalmente, TimeCardView se puede configurar la interfaz con el software de contabilidad de back-end, tales como QuickBooks de Intuit para que los datos del parte de horas puede ser transferido a la perfección el sistema de contabilidad.

NOTA TimeCardView no se admite en todos los modelos de teléfonos IP de Cisco. El número máximo de usuarios de TimeCardView se restringe al máximo de usuarios que admita su plataforma SBCS de Cisco.

Documentación de TimeCardView

Estas guías de TimeCardView están disponibles en Cisco.com:

- Para obtener información detallada sobre la configuración de la aplicación TimeCardView y la administración de usuarios, consulte la guía GUI de *TimeCardView 7.0*.
- Información e instrucciones para usuarios finales se documentan en la *Guía de inicio rápido de TimeCardView 7.0 para usuarios*.

Requerimientos de la plataforma SBCS

- Cisco Configuration Assistant (CCA) 2.0 ó posterior
- Paquete de software para UC500 7.0(3) ó posterior
  - IOS 12.4(20)T2 ó posterior
  - Cisco Unified Communications Manager Express (CME) 7.0 ó posterior
  - Unity Express de Cisco (CUE) CUE 7.0.1 ó posterior

Configuración de TimeCard

En la ficha TimeCard, configure la configuración de administración de la aplicación TimeCardView como se describe a continuación. Haga clic en **Aceptar** o en **Aplicar** cuando haya finalizado de hacer cambios.

Configuración	Descripción
Sesiones máximas	Número máximo de sesiones de TimeCardView, ya sean 2 ú 8, dependiendo de la plataforma. El valor por defecto es 2.
Correos electrónicos de notificación	Dirección de correo electrónico compatible con RFC-2822 que se utilizará para los correos de electrónicos de notificación de la aplicación, por ejemplo, nombre@empresa.com.
Límite de tiempo de la aplicación de teléfono IP de supervisor (60 - 600 segundos)	Lapso de tiempo, en segundos, que transcurre antes que el sistema cierre automáticamente la sesión del supervisor especificado.

Configuración	Descripción
Límite de tiempo de la aplicación de teléfono IP de empleado (60 - 600 segundos)	Lapso de tiempo que transcurre antes que el sistema cierre automáticamente la sesión del empleado especificado.
Duración máxima del trabajo diario (1 - 1440 minutos)	Número de minutos que los empleados pueden permanecer en el estado de trabajo.
Duración máxima de las horas extraordinarias diarias (0 - 1440 minutos)	Máximo de minutos de horas extraordinarias al día que los empleados pueden trabajar. Si se cambia el valor por defecto, no se debe olvidar limitar el número de horas de trabajo normales, de lo contrario, los empleados no podrán acumular horas extraordinarias. El valor por defecto es 0.
Duración máxima del trabajo del turno diario (1 - 1440 minutos)	Número de minutos que los empleados pueden permanecer en el estado de trabajo. El valor por defecto es 1440.
Duración máxima del descanso diario (1 - 1440 minutos)	Número de minutos que los empleados pueden permanecer en el estado de descanso. El valor por defecto es 1440.
Duración máxima del almuerzo del turno diario (1 - 1440 minutos)	Número de minutos que los empleados pueden permanecer en el estado de almuerzo. El valor por defecto es 1440.
Trabajo comienza el	Día de inicio de la semana laboral. Por defecto es lunes.

Configuración del servidor de nóminas

En la ficha Configuración del servidor de nóminas, complete los campos como se describe a continuación si desea integrar TimeCardView con Quick Books de Intuit. Haga clic en **Aceptar** cuando haya finalizado de configurar al servidor.

Configuración	Descripción
Consiguración del servidor de Quick Books	
Su nombre de host	Servidor de nóminas de QuickBooks Nombre de DNS o dirección IP del servidor de nóminas.
Puerto	Número de puerto del servidor de nóminas de QuickBooks. El valor por defecto es 57343.
Horarios de sincronización	
Día de la semana	Día de la semana para la sincronización programada de los datos de TimeCardView con QuickBooks. Por defecto: Diariamente
Hora del día (HH:MM 24 horas)	Hora del día para la sincronización programadas. Por defecto: (ninguno) Ejemplo: 23:00
Hojas de horarios incluidas	Si se incluyen todas las hojas de horario o sólo aquellas aprobadas. Seleccione Todas o Aprobadas. Por defecto: Todas las hojas de horario
Purgar horarios	
Número de días entre purgas	Númer mínimo de días entre las purgas de la base de datos. Intervalo: 1 - 365 días Por defecto 90
Días que se conserva	Mínimo de días que el sistema debe conservar los datos. Intervalo: 1 - 365 días Por defecto 90

18

Mantenimiento

Esta sección cubre estas tareas de mantenimiento que pueden realizarse utilizando Configuration Assistant:

- **Paquetes de localización y software para UC500 de Cisco**
- **Ver información de versión de software y propiedades del dispositivo**
- **Actualizaciones de software**
- **Actualización de correo de voz (UC560)**
- **Administración de archivos**
- **Reiniciar / Restablecer dispositivos**
- **Cómo localizar el UC500 (localizaciones diferentes a Inglés de EE.UU.)**
- **Administración de licencias**
- **Administración de cargas telefónicas**

Consulte **Copia de seguridad y restauración de configuración del dispositivo, página 119** para obtener instrucciones sobre cómo utilizar las funciones de copia de seguridad y restauración disponibles en el elemento Mantenimiento de la barra de funciones.

Paquetes de localización y software para UC500 de Cisco

Lea estas secciones para saber más acerca de los paquetes de localización y software para el UC500:

- **Paquetes de software de UC500**
- **Paquetes de software para el UC500**
- **Descarga de paquetes de localización y software para UC500 de Cisco**

Paquetes de software de UC500

Los paquetes de software pare el UC500 son grandes archivos .ZIP que contienen todos los archivos necesarios para la plataforma de la serie UC500 y su localización. La localización por defecto de fábrica para el UC 500 es Inglés de Estados Unidos.

Paquetes de software para el UC500 separados se entregan para las plataformas modelos UC520, UC540 y UC560. Se debe descargar el archivo .ZIP correcto para su plataforma de UC500.

El paquete de software para el UC500 agrupa todos los archivos necesarios para la plataforma con los archivos de idioma y de teléfonos que se necesitan para la localización por defecto, que es Inglés de Estados Unidos. Los archivos se llaman UC5xx_8.1.0 .zip.

Un archivo .ZIP del paquete de software contiene múltiples archivos TAR y otros para el componente del UC500, incluyendo la:

- Imagen IOS de Cisco para la plataforma UC500
- Archivos de firmware de teléfonos IP de Cisco
- Archivos de soporte de Communications Manager Express (CME)
- Software de correo de voz Unity Express de Cisco (CUE)
- Configuraciones por defecto de fábrica para todas las SKU
- Archivos de soporte, tales como solicitudes y comandos de ACD básica, tonos de llamada e imágenes de escritorio
- Archivos de localización por defecto de fábrica (Inglés de Estados Unidos):
  - Archivos de idioma y regionales para teléfonos
  - Archivos de idioma para el correo de voz

Consulte las *Notas de la versión para Configuration Assistant de Cisco* para ver la compatibilidad e información de la versión para los paquetes de software para el UC500.

Paquetes de software para el UC500

Los paquetes de localización para el UC500 también pueden descargarse para esta ubicación. Los paquetes de localización contienen el software necesario para localizar el correo de voz y los teléfonos (localizaciones para los teléfonos modelos 79xx, SPA525, SPA50x y CP-52x de Cisco).

Esto significa que sólo se necesita descargar un archivo para localizar el correo de voz y todos los modelos de teléfonos admitidos.

Un paquete de localización puede proveerse al instalar software en el UC500 por medio de CCA para instalar un idioma alternativo en el UC500. Pueden instalarse hasta dos idiomas, uno activo y otro alternativo.

Para obtener más información, consulte **Instalación de software del UC500, página 556**.

Descarga de paquetes de localización y software para UC500 de Cisco

Use uno de los siguientes métodos para descargar un paquete de software para el UC500 o un paquete de localización:

- En CCA, seleccione **Conexión de socios** > **Descargas de software para el UC500** de la barra de funciones.
- Abra un navegador web y visite esta URL:

  www.cisco.com/web/go/uc500swpk

Los usuarios que tengan un Contrato de servicios con Cisco válido son elegibles para acceder las versiones actuales y futuras de software desde Cisco (si es que Cisco las deja disponibles). Los socios que no hayan comprado un Contrato de servicios para el UC500 de Cisco son elegibles para descargar la versión actual del software de UC500 dentro de 30 días de la compra del producto de Cisco o de un Socio Cisco autorizado. Esto le da a los usuarios una forma de obtener una versión actual del software para el UC500 para la implementación inicial del producto.

El acceso al software para este propósito necesita una cuenta válida en Cisco.com. Cualquier actualización futura del software (si Cisco la dejara disponible) más allá del período de 30 días desde la compra original necesita un contrato de servicios válido.

Ver información de versión de software y propiedades del dispositivo

Hay varias ubicaciones donde se puede ver la información de versión para el software SBCS en el UC500, así como firmware para los dispositivos conectados.

- El elemento Estado del sistema en el Tablero muestra la versión de la IOS de Cisco.
- Seleccione **Monitorear** > **Telefonía** > **Paquete de software** para ver la información de la versión para el paquete de software de UC500 instalado actualmente, incluyendo la versión de la IOS de Cisco, CME, y CUE, cargas de firwmare telefónico admitidas y resultado del estado de CUE.
- Haga clic con el botón derecho en la vista Topología para mostrar las propiedades del dispositivo, incluyendo el nombre de host, direcciones IP y MAC y la versión del software (por ejemplo, imagen de IOS de Cisco) para el dispositivo.

  Cuando se hace clic con el botón derecho en un teléfono IP, también se ve el tipo de teléfono (modelo), su estado, el nombre y apellido de su usuario, tipos de botones, anexos y etiquetas del botón.

Actualizaciones de software

Para abrir la ventana Actualizar software, seleccione **Mantenimiento** > **Software Actualizar** en la barra de funciones.

- Para saber más acerca de la actualización de software para dispositivos que sean parte de su sitio de clientes, como switches, puntos de acceso inalámbricos, routers o dispositivos de seguridad, consulte **Actualización del firmware del dispositivo, página 552**.
- Para saber más acerca de la actualización del software en el UC500, consulte **Instalación de software del UC500, página 556**.

Actualización del firmware del dispositivo

Aparece la ventana Actualización de VPN cuando se selecciona **Mantenimiento** > **Actualización de software** > **Router/Switch/Seguridad** en la barra de funciones de CCA.

Para saber más acerca de la actualización de software en los dispositivos que CCA gestiona en el sitio del cliente, consulte estos temas:

- **Información sobre la ventana Actualización de Software**
- **Procedimientos**

Información sobre la ventana Actualización de Software

Esta tabla explica las columnas en la ventana Actualización de software.

Columna	Explicación
Dispositivo	Muestra los iconos de dispositivos y nombres de host.
Actualización	Marque la casilla de verificación de Actualización para indicar el o los dispositivos que se van a actualizar cuando se haga clic en **Actualizar**. Puede seleccionar más de un dispositivo del mismo tipo.
Tipo de dispositivo	Muestra el tipo de dispositivo.
Versión actual	Muestra la versión del software que está instalado en el dispositivo.
Nuevo nombre de imagen	Muestra el nombre de la imagen del software que usted proporcionó en la ventana Configuración de actualización. Sólo aparece el nombre del archivo; no la ruta.
Estado de actualización	Si no especificó la configuración de actualización de software, este campo muestra el mensaje "Haga clic en el botón Configuración de actualización para continuar." Una vez que se comience con la instalación, el campo muestra mensajes del estado y progreso de la actualización. Consulte **Mensajes de estado de actualización, página 558** para obtener mayores detalles.

Procedimientos

Antes de comenzar, descargue los archivos de imagen del software que desea instalar.

Siga estos pasos para instalar o actualizar el software en los dispositivos del sitio de clientes de CCA.

PASO 1 En la ventana Actualización de software, seleccione uno o más dispositivos de la misma plataforma.

PASO 2 Haga clic en **Actualizar configuración**.

PASO 3 Complete la ventana Actualizar configuración y haga clic en **Aceptar** para guardar sus entradas. Consulte **Actualizar configuración, página 555**.

PASO 4 Si desea actualizar más de un tipo de dispositivo, repita los Pasos 1 a 4 para cada uno de los tipos de dispositivos.

PASO 5 Marque la casilla **Actualizar** al lado de cada dispositivo que desea actualizar.

PASO 6 Haga clic en **Actualizar** para iniciar el proceso de actualización.

PASO 7 Haga clic en **Estado** para mostrar la ventana Estado de actualización de software. Esta ventana muestra el progreso de la actualización.

Cuando se completa el proceso de actualización de software para todos los dispositivos seleccionados, aparece un diálogo de confirmación. Los mensajes de estado indican cuáles dispositivos se actualizaron con éxito y cuáles no. Consulte **Mensajes de estado de actualización, página 558**.

PASO 8 Haga clic en **Aceptar**. Se le solicita recargar los dispositivos actualizados correctamente.

PASO 9 Seleccione **Sí** para recargar; seleccione **No** si no desea recargar los dispositivos. Los dispositivos no utilizan la actualización hasta que es cargada.

PASO 10 También puede hacer clic en **Recargar dispositivos actualizados** para recargar los dispositivos seleccionados después de haber sido actualizados.

Todos los cambios de configuración se guardan automáticamente en la memoria flash. Después de un minuto, los dispositivos son reiniciados y la nueva imagen comienza a funcionar. Luego puede cerrar la ventana Actualizar software.

- Se puede gestionar los dispositivos en el sitio del cliente tan pronto como sean reiniciados.
- Usted pierde conectividad a un dispositivo cuando lo reinicia.

Actualizar configuración

Esta ventana aparece cuando usted selecciona uno o más dispositivos en la ventana Actualización de software y hace clic en **Actualizar configuración**. Utilícela para especificar la configuración de actualización para dispositivos de la misma plataforma.

Configure la la configuración de actualización como se describe en esta tabla. Haga clic en **Aceptar** cuando esté listo para continuar con la actualización o haga clic en **Cancelar**.

Configuración	Descripción
Dispositivo	Sólo lectura. Muestra el nombre del dispositivo seleccionado.
Imagen	Haga clic en **Explorar** para ubicar la imagen de software que se usará para la actualización.
Modo	En algunos dispositivos se puede seleccionar el modo **Estándar** o **TFTP**. ▪ En modo *estándar* si las imágenes de actualizaciones se guardan localmente. ▪ En el modo *servidor TFTP remoto*, las imágenes de software para la actualización se guardan remotamente. Para actualizar utilizando el modo servidor TFTP remoto, se necesita un servidor TFTP dedicado en una estación de trabajo UNIX o en otra PC. Puede ejecutar cualquier aplicación TFTP de terceros en el servidor remoto. Si seleccionó **Servidor TFTP remoto**: ▪ En el campo **Archivo de imagen**, especifique la ruta completa y el nombre del archivo de la imagen IOS de Cisco. ▪ En el campo **Dirección IP del servidor TFTP** , especifique la dirección IP de su servidor TFTP. Se puede seleccionar múltiples miembros del sitio y actualizar sus imágenes IOS de Cisco. Para realizar actualizaciones de grupo, su servidor TFTP debe manejar múltiples solicitudes y sesiones simultáneamente.

Instalación de software del UC500

Aparece el Asistente de instalación de software para el UC500 cuando se selecciona **Mantenimiento** > **Actualización de software** > **UC500**.

Para saber más acerca de la preparación para una instalación de software para el UC500, consulte estos temas:

- **Asistente de instalación de software para el UC500**
- **Preparación de la instalación de software del UC500**
- **Mensajes de estado de actualización**

PRECAUCIÓN Cisco no recomiendas que se realicen actualizaciones de software en una conexión WAN remota. Si se interrumpe la conexión a la WAN, fallará la operación y el sistema o dispositivo puede quedar inutilizable.

Asistente de instalación de software para el UC500

Usando el Asistente de instalación de software para el UC500, se puede:

- Instalar un paquete de software al UC500

  Esta es la forma preferida para instalar y actualizar el software para el UC500. Al usar este método, seleccione **Todo** al seleccionar la configuración de actualización. El paquete de software para el UC500 incluye las cargas de teléfonos CME relacionadas con CUE, IOS de Cisco, comandos para Contestadora automática, archivos de idioma y localización de Inglés de Estados Unidos para teléfonos y correo de voz y archivos de soporte.

- Instalar un paquete de localización en el UC500
- Sólo actualice la imagen del software de IOS de Cisco en el UC500
- Sólo actualice el software de correo de voz de CUE en el UC500

NOTA Al descargar las imagen específica de IOS o CUE desdeCisco.com, utilice la versión .tar de las imágenes IOS de Cisco y el archivo de paquete de CUE para el software de correo de voz de CUE.

Siga las instrucciones en pantalla del asistente para instalar el software.

Preparación de la instalación de software del UC500

Para evitar fallos en la actualización e instalación del software, así como otros problemas, lea esta sección con cuidado y verifique que el sistema esté listo para la actualización o instalación realizando estas tareas.

- Verifique que su PC cumpla los requerimientos para utilizar CCA. Consulte **Requerimientos del sistema, página 17**.
- Si se tiene una NIC (tarjeta de interfaz de red) dual en la PC que ejecuta Configuration Assistant, asegúrese que sólo una de las interfaces esté activada.
- Apague los servicios FTP/TFTP que se ejecuten en su PC.

  Antes de actualizar, desactive cualquier servidor TFTP de terceros que se ejecute en su PC local. El servidor TFTP integrando en CCA se utiliza para transferir imágenes y archivos desde su PC a la interfaz que se va a actualizar. Sólo un servidor TFTP puede tener acceso al puerto TFTP a la vez.

  En la PC que ejecuta CCA, abra una ventana de comandos y ejecute el comando `netstat -a` para ver si se está ejecutando algun servicio FTP o TFTP. No debería ver el puerto 21, 69, FTP ni TFTP en la salida. Si ellos están, apague esos procesos o servicios.

  Si no hay servicios TFTP de terceros ejecutándose, intente reiniciar su PC para liberar puertos TFTP que aún pueden estar en uso desde una sesión anterior de CCA.
- Asegúrese que la PC haya obtenido una dirección DHCP del UC500 y que el gateway por defecto está configurado correctamente.

  En la PC que ejcuta CCA, abra una ventana de comandos y ejecute el comando `ipcongif /all`. La dirección IP del gateway por defecto indicada en la salida debería obtenerse desde el UC500 (el valor por defecto es 192.168.10.1).
- Cualquier software de firewall instalado en la PC que ejecuta CCA debe configurarse para que permita el acceso TFTP y FTP hacia y desde el UC500.

  Un firewall ejecutándose en su PC puede potencialmente bloquear la conexión entre el módulo CUE en el UC500 y CCA, lo que puede ocasionar un fallo de la actualización.

Si se desactiva el firewall que se ejecuta en la PC mientras se realiza la actualización, asegúrese de volver a activarlo después de la actualización.

- Verificación del estado de la interfaz CUE. Para hacer esto, seleccione **Solución de problemas** > **Diagnóstico de CUE > Diagnóstico de conectividad de CUE** en la barra de funciones y haga clic en **Verificar estado**. Se debería ver la línea "`Integrated-Service-Engine0/0 está activado, protocolo de línea está activado`" en la sección "mostrar interfaces" cerca de la parte superior de la salida si el módulo de la interfaz CUE está ejecutándose.

Estado de actualización de software

Esta ventana aparece cuando selecciona un dispositivo y hace clic en **Estado** en la ventana Actualización de software. La ventana muestra mensajes detallados a medida que se generan desde el dispositivo durante una actualización.

Si no hay espacio suficiente en el dispositivo para instalar la nueva imagen, aparece un mensaje con un enlace a la ventana Administración de archivos. Puede utilizar la ventana Administración de archivos para administrar los archivos del sistema y, si es necesario, eliminar las imágenes antiguas para liberar espacio para las nuevas imágenes.

Mensajes de estado de actualización

Esta tabla explica los mensajes de estado de actualización.

Mensaje	Explicación
Haga clic en el botón Actualizar configuración para continuar	La ventana Actualizar configuración se debe completar antes de actualizar el dispositivo.
Haga clic en el botón Actualizar para actualizar el dispositivo.	Todos los parámetros se configuran para el dispositivo a actualizar.
Recarga iniciada para el dispositivo.	El dispositivo se recarga después de una actualización de software exitosa. Incluso después de completar la recarga, este mensaje aparece hasta que usted actualiza la ventana.
La actualización de software fue correcta.	Se completó exitosamente la actualización.

Mensaje	Explicación
Error al actualizar software	Error al actualizar. Vea la ventana Estado para obtener más información. **IMPORTANTE** Si falla una actualización de UC500, verifique que se hayan realizado todas las tareas indicadas en la **Preparación de la instalación de software del UC500, página 557**.
Actualización de software en progreso.	La actualización de los dispositivos está en proceso.
Cargando la imagen	La imagen se carga al dispositivo.
Verificación de la imagen	El dispositivo está verificando la imagen.

Actualización de correo de voz (UC560)

La plataforma UC560 admite la actualización de la memoria flash compacta del correo de voz desde el tamaño por defecto de 2 GB a 4 GB ó a 8 GB para aumentar la capacidad de almacenamiento de correo de voz. Una vez que se reemplace la memoria flash compacta y se reinicie el UC560, se le solicitará que instale los archivos de software del correo de voz y los de idioma en la nueva memoria flash del correo de voz.

Consulte estas seccones para obtener más información:

- **Preparación de una Actualización de correo de voz**
- **Reemplazo de la memoria flash del correo de voz en el UC560 y ejecución de una actualización de correo de voz**

Preparación de una Actualización de correo de voz

Antes de realizar una actualización de correo de voz:

- Si se tiene una NIC (tarjeta de interfaz de red) dual en la PC que ejecuta Configuration Assistant, asegúrese que sólo una de las interfaces esté activada.
- Cualquier software de firewall instalado en la PC que ejecuta CCA debe configurarse para que permita el acceso TFTP y FTP hacia y desde el UC500.

- Apague cualquier servidor TFTP o FTP de terceros que se ejecute en la PC que ejecuta CCA.
- Si no hay servicios TFTP de terceros ejecutándose, intente reiniciar su PC para liberar puertos TFTP que aún pueden estar en uso desde una sesión anterior de CCA.
- Si el UC500 no está en estado por defecto de fábrica:
  - Guarde la configuración en ejecución como la configuración de inicio. Consulte **Aplicar y guardar la configuración, página 50**.
  - Haga copia de seguridad de la configuración actual del UC500 y **Copia de seguridad y restauración de configuración del dispositivo, página 119**.
- Asegúrese de haber descargado el paquete de software para UC500 más reciente para la plataforma UC500 (por ejemplo UC560-8.1.0.zip ó posterior) en la PC que está ejecutando CCA. El paquete de software contiene el último software para correo de voz de CUE (archivo SCUE*.zip).
- Si se necesita una localización distinta a Inglés de Estados Unidos o desea instalar archivos para una localización alternativa, también se debe descargar los paquetes de localización para UC500 adecuados. Consulte **Paquetes de software para el UC500, página 551**.

  Para descargar los paquetes de localización para el UC500, vaya a: www.cisco.com/go/uc500swpk.
- Si se desea, descargue copias de los archivos personalizados desde la memoria flash del UC500 a su PC usando la ventana Administración de archivos de CCA (**Mantenimiento** > **Administración de archivos**. Consulte **Administración de archivos, página 574**.

Reemplazo de la memoria flash del correo de voz en el UC560 y ejecución de una actualización de correo de voz

Una memoria flash de mayor capacidad para el correo de voz del UC560 puede pedirse a Cisco como repuesto (UC500-8GB= para la memoria de 8-GB y UC500-4GB= para la de 4-GB).

ADVERTENCIA Antes de instalar una nueva memoria flash compacta de correo de voz en el UC560, se debe guardar y hacer copia de seguridad de la configuración del UC560 y, luego, apagar el UC560. Si ello no se hace se puede hacer que el sistema quede inoperativo o se pierdan datos.

Para reemplazar la memoria flash para el correo de voz del UC560 y ejecutar una actualización del correo de voz usando CCA, realice estos pasos.

PASO 1 Asegúrese de haber realizado las tareas indicadas en **Preparación de una Actualización de correo de voz, página 559**.

PASO 2 Apague el UC560.

PASO 3 Ubique la ranura de la memoria flash para el correo de voz y retire la memoria flash existente.

PASO 4 Inserte la nueva memoria flash en la ranura vacía.

PASO 5 Encienda el UC560.

PASO 6 Con la PC ejecutando CCA conectada al lado de LAN del UC500, inicie CCA y conéctese al UC560.

CCA detecta que se instaló una nueva memoria flash para el correo de voz, muestra un mensaje informando que no hay software de correo de voz de CUE instalado y pregunta si se desea instalarlo.

- Si se selecciona **Sí**, aparece la ventana Asistente de instalación de software para el UC500.
- Si se selecciona **No** o se cierra la ventana, siempre se puede volver a abrirla desde la barra de funciones seleccionando **Mantenimiento** > **Actualización de software** > **UC500**.

Debido a que la nueva memoria flash no tiene un software ni datos en ella, las funciones de correo de voz no están disponibles en el sistema hasta que se instale el software del correo de voz.

PASO 7 Siga las instrucciones en pantalla en el Asistente de instalación de software para el UC500 para instalar los archivos de idioma y software de correo de voz. Cuando se le pida seleccionar una opción de instalación, seleccione **Software de correo de voz**.

El proceso de actualización tarda aproximadamente 30 minutos.

CCA realiza una restauración desde la copia de seguridad más reciente del correo de voz una vez que se termina la instalación del software.

PASO 8 Para verificar que la instalación del software del correo de voz se finalizó con éxito

- Abra la ventana Correo de voz (**Configurar** > **Telefonía** > **Correo de voz**) y verifique que los datos de almacenamiento de correo de voz disponibles reflejen la mayor capacidad.
- Haga llamadas, deje mensajes en el correo de voz y recupérelos para verificar que el sistema de correo de voz funcione según lo esperado.
- Recupere correo de voz existente para verificar que los mensajes antiguos seas accesibles según lo esperado.

PASO 9 Guarde la configuración (**Configurar** > **Guardar configuración**).

PASO 10 Haga una copia de seguridad de la nueva configuración (**Mantenimiento** > **Archivo de configuración**, **Copia de seguridad**).

.

Administración de licencias

Para administrar licencias, seleccione **Mantenimiento** > **Administración de licencias** en la barra de funciones.

Las opciones de administración de licencias difieren entre las plataformas UC520 y UC540. Estas opciones se analizan con mayor detalle en estas secciones:

- **Visión general, página 562**
- **Tipos de licencias, página 563**
- **Administración de licencias de UC520, página 564**
- **Administración de licencias de UC540 y UC560, página 566**

Visión general

Las licencias de software de Cisco se admiten en las plataformas de la serie UC500 para que puedan modificarse en terreno. Por ejemplo, un sistema licenciado para 8 usuarios que físicamente admite 16 usuarios puede actualizarse a una licencia de 16 usuarios. Las licencias también pueden degradarse.

Se registran los teléfonos IP, según la disponibilidad de una licencia para cada teléfono. En las plataformas UC520, cuando un sistema de licencias se degrada debido al vencimientos de las licencias o por una configuración del usuario y el número de teléfonos registrados supera al límite de licencias de usuarios, el sistema se recarga.

Están disponibles las siguientes funciones de licencia de software:

- Para la plataforma UC520, se admiten licencias de evaluación, extensión, permanentes y de periodos de gracia.
- Para las plataformas UC540 y UC560, se admiten licencias de evaluación y permanentes. Las plataformas UC540 y UC560 admiten las actualizaciones de licencias con Clave de autorización de productos (PAK).
- Los eventos de instalación y vencimiento se administración por medio de la infraestructura de licencias.

Tipos de licencias

Configuration Assistant admite cuatro tipos de licencias, las que se describen en esta sección.

Tipo de licencia	Descripción
Licencia de evaluación	Las licencias de evaluación son licencias medidas y no bloqueadas por nodos, que se agrupan con una imagen de IOS y que son válidas por un período limitado. La licencia sólo se usa cuando no hay licencias permanentes, de extensión ni de periodos de gracia para una función. Se debe aceptar el EULA (Acuerdo de licencia de usuario final) antes de utilizar esta licencia. Cada vez que se conecte o actualice la red, Configuration Assistant le notifica del estado de una licencia temporal utilizando la ventana Notificación de eventos. También se le notifica si la licencia para cualquier función vence dentro de 10 días ó menos y el sistema le recomienda que instale una licencia permanente.

Tipo de licencia	Descripción
Licencia permanente	Las licencias permanentes son licencias no bloqueadas por nodos sin un periodo de utilización asociado, otorgadas por medio del portal de licencias de Cisco. Para las plataformas UC520, se debe aceptar el EULA como parte de la instalación de la licencia.
Licencia de extensión	Sólo UC520. Las licencias de extensión son licencias medidas no bloqueadas por nodos, otorgadas por medio del portal de licencias de Cisco. Para las plataformas UC520, se debe aceptar el EULA como parte de la instalación de la licencia.
Licencia de periodo de gracia	Sólo UC520. Las licencias de periodos de gracia son licencias medidas bloqueadas por nodos, otorgadas por medio del portal de licencias de Cisco como parte del permiso para volver a tener una licencia en el host. Estas licencias se instalan en el dispositivo como parte de la operación para estar nuevamente en el host. Se debe aceptar el EULA como parte de esta operación para este tipo de licencia.

Administración de licencias de UC520

Para ver la información de licencias o para instalar una, seleccione **Mantenimiento** > **Administración de licencias** en la barra de funciones.

Esta tabla indica y describe la información de licencias del UC520 que se muestra en esta ventana.

Configuración	Descripción
Dispositivo/Función	Muestra los dispositivos disponibles y las licencias de usuarios instaladas actualmente.
ID de dispositivo	Sólo lectura. Muestra el identificador único del dispositivo para el UC520. Por ejemplo: UC520W-FXO-K9:FFH104001MR.
Capacidades actuales	Número actual de las licencias de usuarios instaladas en este UC520.
Capacidades máximas	Número máximo de las licencias de usuarios admitidas en este UC520 SKU.

Configuración	Descripción
Tipo de licencia	La licencia puede ser permanente, de evaluación, de extensión o de periodo de gracia.
Periodo de vencimiento	Para las licencias permanentes, siempre aparece la frase De por vida para el periodo de vencimiento. Para las licencias de evaluación, el Periodo de vencimiento es el tiempo restante hasta que venza la licencia de evaluación.
Acción	Las opciones disponibles incluyen **Ninguna** o **Seleccionar archivo de licencia**.

Para instalar una licencia de **evaluación**, siga estos pasos:

PASO 1 En la ventana Administración de licencias, haga clic en el dispositivo UC500 para el que desee ver o instalar la licencia de evaluación.

PASO 2 En la lista Acción del dispositivo, seleccione **Licencia de evaluación**.

PASO 3 Haga clic en **Aceptar** o **Aplicar** para instalar las licencias. Se actualizan los campos relacionados.

Para instalar una licencia **permanente** o una **de extensión**, siga estos pasos:

PASO 1 En la lista Acción del dispositivo, seleccione **Seleccionar archivo de licencia**. Aparece el diálogo Cargar archivo de licencia.

PASO 2 Haga clic en **Explorar** para navegar hasta la ubicación del archivo de licencia y haga clic en **Aceptar**. Consulte **Cargar archivo de licencias, página 571**.

Para cancelar una actualización de licencia, haga clic en **Cancelar** antes de hacer clic en **Aplicar** o en **Aceptar**. Se cancela la instalación, y aparece el estado original de la licencia.

PASO 3 Haga clic en **Aceptar** o **Aplicar** para instalar la licencia. Se actualizan los campos relacionados.

Cuando las licencias se instalan en forma exitosa, se actualiza la columna Capacidades para reflejar las licencias adicionales.

Administración de licencias de UC540 y UC560

Las licencias de software en las plataformas UC540 y UC560 también admiten el mecanismo PAK (Clave de autorización de productos) para software para las actualizaciones de licencias. Para conocer mayores detalles, consulte la siguiente sección; **Acciones de administración de licencias, página 567**.

Esta tabla indica y describe la información de licencias del UC520 que se muestra en esta ventana.

Configuración	Descripción
Dispositivo/Función	Muestra los dispositivos disponibles y las licencias instaladas actualmente. Las licencias de los dispositivos UC540 y UC560 se indican como Licencias de usuario Pro.
ID de dispositivo	Sólo lectura. Muestra el identificador único del dispositivo para el dispositivo UC540 ó UC560. Por ejemplo: UC540W-FXO-K9:FFH104001MR.
Capacidades actuales	Número actual de las licencias instaladas en este UC540 ó UC560.
Capacidades máximas	Número máximo de licencias admitidas. Para el UC540, es 32. El UC560 admite hasta 104 licencias de usuarios.
Tipo de licencia	Para el UC540 y el UC560, puede ser Permanente o de Evaluación. Las licencias pueden estar Activas o Inactivas.
Periodo de vencimiento	Para las licencias permanentes, siempre aparece la frase De por vida para el periodo de vencimiento. Para las licencias de evaluación, el Periodo de vencimiento es el tiempo restante hasta que venza la licencia de evaluación.

Configuración	Descripción
Acción	Para las licencias activas, haga clic en **Administrar** para abrir la ventana Detalles de administración de licencias, donde se puede instalar, actualizar, transferir, activar o desactivar las licencias. Consulte **Acciones de administración de licencias, página 567**.

Acciones de administración de licencias

Esta ventana aparece cuando se selecciona un UC540 ó un UC560 en la ventana Administración de licencias, se selecciona una licencia y se hace clic en **Administrar**.

Visión general

La plataforma UC540 sale de la fábrica con 8 licencias permanentes instaladas y activas; la plataforma UC560 sale con 16 licencias permanentes instaladas y activas. Estas licencias instaladas en fábrica no pueden transferirse, revocarse ni modificarse.

El número máximo de licencias de usuario para la plataforma UC540 es 32. Para la UC560, el máximo de licencias de usuario es 104. Las licencias adicionales pueden agregarse en grupos de 8 utilizando una Clave de autorización de productos (PAK) o por medio de un archivo de licencias. Si ya se ha instalado el número máximo de licencias, se desactivan las opciones de instalar licencia y actualizar licencia con una PAK.

Los campos de configuración que aparecen en esta ventana varían, dependiendo de la acción de administración de licencias que seleccione. Pueden realizarse las siguientes acciones:

- **Actualizar licencia utilizando una PAK (Clave de autorización de productos), página 568**
- **Transferir licencias hacia o desde este dispositivo, página 569**
- **Instalar licencia desde el archivo, página 571**
- **Activar o desactivar una licencia de evaluación, página 571**

Actualizar licencia utilizando una PAK (Clave de autorización de productos)

Seleccione la opción **Actualizar licencia utilizando una PAK (Clave de autorización de productos)** si desea instalar licencias adicionales utilizando una PAK. Esta opción no está disponible si ya se ha instalado el número máximo de licencias.

Se contacta y actualiza la base de datos SWIFT (Tecnología de Infraestructura y cumplimiento de software) cuando se actualizan las licencias.

Para instalar una licencia actualizada utilizando una PAK, siga estos pasos:

PASO 1 En la sección **Acciones** de la ventana, seleccione **Actualizar licencia utilizando una PAK (Clave de autorización de productos)**.

La ID del dispositvo de la parte superior de la ventana muestra la ID única para este dispositivo UC540.

PASO 2 En la sección **Detalles de acciones** de la ventana, complete la configuración como se describe a continuación.

Configuración	Descripción
Usuario de Cisco.com	Especifique su ID de usuario de Cisco.com.
Contraseña de Cisco.com	Especifique su contraseña de Cisco.com.
Dirección de correo electrónico	Especifique una dirección de red válida. Esta se la dirección a la que se envían los correos electrónicos de notificación desde SWIFT.
Número de PAK a instalar	Seleccione el número PAK (Clave de autorización de productos) a instalar de la lista desplegable; desde 1 a 3 para el UC540 ó de 1 a 8 para el UC560.
PAK-1 hasta PAK-3 (UC540) **PAK-1 hasta PAK-8 (UC560)**	Especifique la Clave de autorización de productos para cada licencia que se va a instalar.

PASO 3 Haga clic en **Aceptar** para cerrar la ventana Acciones de administración de licencias y volver a la ventana Administración de licencias.

Transferir licencias hacia o desde este dispositivo

Seleccione **Transferir licencias hacia o desde este dispositivo** si desea:

- Revocar y eliminar licencias de este dispositivo UC540 ó UC560 y guardarlas en un archivo, o
- Transferir las licencias guardadas previamente en otro dispositivo UC540 ó UC560.

Cuando se eliminan licencias de un UC540 ó UC560:

- Las licencias se guardan en un archivo en la PC que ejecuta Configuration Assistant.
- La ubicación se muestra en la ventana Acciones de administración de licencias.

Cuando se transfiere la licencia a un UC540 ó UC560 diferente, asegúrese que el archivo esté presente en la PC que ejecuta Configuration Assistant. Utilice la misma PC para eliminar y transferir las licencias o copiar el archivo de licencias guardadas en la misma ubicación en la PC que se va a usar para la transferencia de licencias.

Se contacta y actualiza la base de datos SWIFT (Tecnología de Infraestructura y cumplimiento de software) cuando se revocan y transfieren las licencias.

Para eliminar licencias de un UC540 ó UC560 para transferirlas a otro UC540 ó UC560, siga estos pasos.

PASO 1 En la sección **Acciones** de la ventana Acciones de administración de licencias, seleccione**Transferir licencias hacia o desde este dispositivo.**

PASO 2 En la sección **Detalles de acciones** de la ventana, complete la configuración como se describe a continuación.

Configuración	Descripción
Nombre de usuario de Cisco.com	Especifique su ID de usuario de Cisco.com.

Configuración	Descripción
Contraseña de Cisco.com	Especifique su contraseña de Cisco.com.
Dirección de correo electrónico	Especifique una dirección de red válida. Esta se la dirección a la que se envían los correos electrónicos de notificación desde SWIFT (Tecnología de Infraestructura y cumplimiento de software).
Tipo de transferencia	Seleccione **Eliminar licencia y guardar para transferencia**.

PASO 3 Cuando se hace clic en **Aceptar**, el sistema se conecta a la base de datos SWIFT y revoca la licencia. La licencia es eliminada del UC540 ó UC560 y se guarda en un archivo en la PC que ejecuta Configuration Assistant.

La ubicación del archivo en la PC local se muestra en la ventana Acciones de administración de licencias.

Para instalar una licencia guardada previamente y transferida de otro UC540 ó UC560, siga estos pasos.

PASO 1 En la sección **Acciones** de la ventana, seleccione**Transferir licencias hacia o desde este dispositivo.**

PASO 2 En la sección **Detalles de acciones** de la ventana, complete la configuración como se describe a continuación.

Configuración	Descripción
Nombre de usuario de Cisco.com	Especifique su ID de usuario de Cisco.com.
Contraseña de Cisco.com	Especifique su contraseña de Cisco.com.

Configuración	Descripción
Tipo de transferencia	Seleccione **Transferir la licencia guardada previamente**. Seleccione la licencia a instalar del menú de la lista desplegable **Licencias descubiertas**. Al descubrir licencias, Configuration Assistant sólo busca en la ubicación en la que la licencia estaba guardada previamente.

PASO 3 Haga clic en **Aceptar** para instalar la licencia y cerrar la ventana Acciones de administración de licencias. Se regresa a la ventana Administración de licencias.

Instalar licencia desde el archivo

Seleccione **Instalar archivo de licencia** si desea instalar manualmente una licencia utilizando un archivo de licencia.

Para instalar una licencia desde un archivo, siga estos pasos.

PASO 1 En la sección **Acciones** de la ventana, seleccione **Instalar licencia desde archivo**.

PASO 2 En la sección **Detalles de la acción** de la ventana, haga clic en **Explorar** y ubique el archivo de licencias que se va a instalar, luego, haga clic en **Aceptar**. Consulte **Cargar archivo de licencias, página 571**.

PASO 3 Haga clic en **Aceptar** o en **Aplicar**para instalar la licencia y cerrar la ventana Acciones de administración de licencias.

Activar o desactivar una licencia de evaluación

Para activar o desactivar una licencia, seleccione **Activar licencia de evaluación** o **Desactivar licencia de evaluación**, luego, haga clic en **Aceptar**. No se necesita otra información.

Cargar archivo de licencias

Aparece el diálogo Cargar archivo de licencias cuando se está administrando licencias en un UC520 y se selecciona **Seleccionar archivo de licencias** de la lista despegable de la ventana Administración de licencias.

Haga clic en **Explorar** para navegar hasta la ubicación del archivo de licencia en su sistema y haga clic en **Aceptar** para cargar el archivo de licencias.

El archivo de licencias tendrá una extensión .lic o .xml.

Reiniciar / Restablecer dispositivos

Para abrir la ventana Reiniciar/Restablecer, seleccione **Mantenimiento** > **Reiniciar/Restablecer** en la barra de funciones.

Visión general

Se puede *reiniciar* dispositivos en su sitio de cliente o *restablecerlos* a sus valores por defecto de fábrica.

- Si se reinicia un dispositivo se guarda el archivo de configuración activa y se inicia nuevamente. Un dispositivo no es accesible mientras se está reiniciando y se interrumpe la conectividad brevemente entre el dispositivo y sus estaciones de extremos.
- Si se restablece un dispositivo, se restablece la configuración que tenía cuando era nuevo de fábrica. Después que un dispositivo se restablece a los valores por defecto de fábrica, se puede utilizar uno de los asistentes de configuración de dispositivos para establecer la configuración o volver a configurar el dispositivo manualmente.

NOTA Cuando se restablezca un dispositivo, el servidor DHCP podría asignar una nueva dirección IP a un dispositivo restablecido. Si ello sucede, la vista Topología CCA muestra que el dispositivo es inalcanzable. Haga clic con el botón derecho en la vista Topología y seleccione **Agregar al sitio** para volver a agregar el dispositivo a su sitio de cliente con su nueva dirección IP.

Procedimientos

Para reiniciar o restablecer un dispositivo en su sitio de cliente, siga estos pasos:

PASO 1 En la ventana Reiniciar/Restablecer, seleccione el dispositivo que desea reiniciar o restablecer.

PASO 2 Seleccione uno de los siguientes pasos:

- Marque la opción **Reiniciar**.
- Marque la opción **Restablecer a valores por defecto de fábrica**.

- Marque ambas opciones.

PASO 3 Haga clic en **Aceptar**.

Para reiniciar CUE

Para el UC500, se puede seleccionar reiniciar sólo el módulo Unity Express de Cisco El correo de voz, la Contestadora automática y otras aplicaciones de telefonía se ejecutan sobre el módulo CUE.

PRECAUCIÓN Sólo se debería reiniciar el módulo CUE si recibe dichas instrucciones de Cisco TAC para abordar un tema específico o si es necesario como parte de una operación relacionada con Configuration Assistant; por ejemplo, forzar una segunda lectura de los archivos de idiomas instalados para la aplicación WebEx PhoneConnect de Cisco.

El reinicio de CUE puede tomar de 10 a 15 minutos. Durante dicho lapso, el correo de voz, la Contestadora automática y otras aplicaciones de telefonía, como WebEx PhoneConnect y TimeCardView de Cisco no están disponibles.

Para reiniciar el módulo CUE, seleccione **Inicio** > **Topología** para abrir la vista Topología , haga clic con el botón derecho en el icono del UC500 en la vista Topología y seleccione **Reiniciar CUE** en el menú.

SUGERENCIA Para acceder a las herramientas de diagnóstico de CUE y de solución de problemas, vaya a **Solución de problemas** > **Diagnóstico de telefonía** > **Diagnóstico de CUE** > **Diagnóstico de conectividad de CUE**. Para obtener más información, consulte **Diagnóstico de conectividad de CUE, página 634**.

Cómo localizar el UC500 (localizaciones diferentes a Inglés de EE.UU.)

La localización del sistema por defecto para el UC 500 es Inglés de Estados Unidos.

Para localizar el UC500, los teléfonos y el correo de voz con una localización diferente, realice estos pasos.

PASO 1 Descarga el último paquete de software para el UC500, si es necesario, y descargue los paquetes de localización para el UC500 para las localizaciones deseadas.

Consulte **Descarga de paquetes de localización y software para UC500 de Cisco, página 551**.

PASO 2 Para instalar los paquetes de localización y software, seleccione **Mantenimiento** > **Actualización de Software** > **UC500** y siga las instrucciones en pantalla.

Consulte **Instalación de software del UC500, página 556**.

PASO 3 En la ventana Plan de numeración saliente, seleccione la localización del plan de numeración que corresponda a la localización deseada o cargue un plan de numeración localizado y personalizado.

Consulte **Plan de numeración saliente, página 473**.

Administración de archivos

Para administrar el sistema de archivos en la memoria flash compacta para el UC500 o el sistema de archivos para otros dispositivos de IOS de Cisco, seleccione **Mantenimiento** > **Administración de archivos** en la barra de funciones.

SUGERENCIA El elemento Utilización de flash en la vista Tablero entrega información acerca del porcentaje de almacenamiento utilizado y disponible en la memoria flash compacta. Para abrir el Tablero, seleccione **Inicio** > **Tablero** en la barra de funciones. Se puede eliminar cargas telefónicas de la memoria flash para liberar espacio, si es necesario. Consulte **Administración de cargas telefónicas, página 580**.

Visión general

En la ventana Administración de archivos, usted puede:

- Visualizar los sistema de archivos de cualquiera de los dispositivos de IOS de Cisco mientras se encuentren conectados a una red activa.
- Realizar operaciones básicas de administración de archivos en estos sistemas de archivos.

- Eliminar archivos de la memoria flash.

  Por ejemplo, cuando se realice una actualización del software, tal vez no se tenga el espacio suficiente para instalar la nueva imagen y, por lo tanto, puede ser necesario eliminar la imagen antigua para dejar espacio para la nueva imagen.

- Carga y descarga de archivos hacia y desde la memoria flash

Procedimientos

La ventana Administración de archivos tiene dos fichas:

- **Visión general**
- **Archivos**

Visión general

Esta tabla explica las columnas de la ficha **Visión general**.

Columna	Explicación
Sistema de Dispositivo / Archivo	Muestra los dispositivos seleccionados y los sistemas de archivos en dichos dispositivos.

Columna	Explicación
Estado	El estado de un sistema de archivos puede ser cualquiera de los siguientes: ▪ **Vacío**—No hay estado que informar. ▪ **Compresión necesaria**—Hay archivos eliminados en un sistema de archivos B. ▪ **Compresión en progreso**—Actualmente se está purgando archivos marcados para la eliminación. ▪ **Sistema de archivos en uso** — No está disponible la información del sistema de archivos. Haga clic en **Actualizar** para intentarlo de nuevo. ▪ **Sistema de archivos completo**—No hay espacio libre en el sistema de archivos. ▪ **Sistema de archivos vacío**—No hay archivos en el sistema de archivos. ▪ **Sistema de archivos es de sólo lectura**—El sistema de archivos está bloqueado y no puede modificarse. Con frecuencia, ello se debe a una configuración física del switch en una tarjeta CompactFlash.
Capacidad	Tamaño del sistema de archivos, redondeado al megabyte (MB) más cercano.
Espacio libre	Megabytes libres en el sistema de archivos, redondeado al MB más cercano.
% de espacio libre	Porcentaje del total del sistema de archivos que no está en uso.
Archivos	Número de archivos en el sistema de archivos. Los directorios de los sistemas de archivos de clase C y los archivos en eliminados en los sistemas de archivos de clase B también se cuentan como archivos.

Archivos

Esta tabla explica las columnas de la ficha **Archivos**.

Columna	Explicación
Sistema de Dispositivo / Archivo	Muestra los dispositivos seleccionados y los sistemas de archivos en dichos dispositivos. Bajo cada sistema de archivos se encuentra una lista de directorios y archivos.
Compresión	Está acción sólo aparece cuando existe un archivo eliminado en un dispositivo con un sistema de archivos de clase B. Marque la casilla proporcionada par eliminar permanentemente los archivos del sistema de archivos. La casilla no está disponible si el sistema de archivos es de sólo lectura, ni en caso que no existan archivos eliminados en el sistema de archivos.
Tamaño	Indica los tamaños de archivos individuales en KB.
Tipo	Indica el tipo de archivos individuales, si lo hubiere. Los tipos de archivos comunes incluyen la Imagen del sistema, la Imagen de IOS de Cisco y Configuración.
Modificado	Indica la fecha y hora de modificación del archivo.
Eliminar	Marque la casilla para seleccionar eliminar un archivo. Si el archivo está en un sistema de archivos de clase B y ya existe un archivo marcado para su eliminación, ya está marcada dicha casilla.
Restaurar	Sólo aparece en el caso de dispositivos que tengan sistemas de archivos de clase B con archivos eliminados. Marque las casillas para seleccionar los archivos que desea eliminar.

Carga, descarga y eliminación de archivos de la memoria flash

Se pueden cargar y descargar archivos hacia y desde la memoria flash compacta en el UC500 u otros dispositivos de IOS de Cisco que CCA administre. Por ejemplo, se puede descargar archivos de tonos telefónicos personalizados, imágenes de escritorio de teléfono, comandos personalizados para la contestadora automática o archivos de soporte según lo indique Soporte de Cisco. Se pueden descargar copias de archivos de la memoria flash hacia su máquina local para guardarlos y cargarlos en otro dispositivo.

IMPORTANTE CCA usa un servicio FTP incorporado para transferir los archivos entre su PC y la memoria flash compacta en el UC500 u otros dispositivos IOS de Cisco que CCA administra. Se debe desactivar cualquier servicio FTP de terceros que se esté ejecutando en la PC antes de poder transferir los archivos. Si no hay servicios FTP de terceros ejecutándose, verifique la configuración de seguridad de la red y del firewall en su PC para asegurarse que se permite el tráfico FTP entre la PC y el dispositivo o intente reiniciar su PC.

Para cargar un archivo de su máquina local hacia la memoria flash compacta en un dispositivo IOS de Cisco, siga estos pasos.

PASO 1 En la ventana Administrador de archivos, seleccione la ficha **Archivos**.

PASO 2 En el árbol **Sistema de dispositivos/archivo**, seleccione el dispositivo y navegue hasta la ubicación de la memoria flash donde desee cargar el archivo.

Asegúrese de cargar el archivo en la ubicación correcta en la memoria flash. Por ejemplo, los archivos de audio para Música en espera se cargan en el directorio `flash:\media`. Para obtener más información, consulte la documentación de CME unificado de Cisco en Cisco.com.

PASO 3 Haga clic en **Cargar**.

Para descargar una copia de uno o más archivos de la memoria flash compacta en un dispositivo IOS de Cisco a su máquina local, siga estos pasos.

PASO 1 En la ventana Administrador de archivos, seleccione la ficha **Archivos**.

PASO 2 En la jerarquía **Sistema de dispositivos/archivo**, seleccione el dispositivo y navegue hasta la carpeta de la memoria flash que contiene el o los archivos que desee descargar.

PASO 3 Haga clic en los nombres de los archivos que desee descargar para seleccionarlos.

Puede presionar el botón izquierdo del mouse junto con la tecla CTRL de Windows o el botón izquierdo del mouse junto con la tecla Shift para seleccionar múltiples archivos.

El botón **Descargar** no está activo hasta que se haya seleccionado al menos un archivo.

PASO 4 Haga clic en **Descargar**.

Para eliminar uno o más archivos de la memoria flash compacta en un dispositivo IOS de Cisco, siga estos pasos.

PRECAUCIÓN No elimine la imagen de arranque del sistema ni ninguno de estos archivos en la memoria flash del UC500: vlan.dat, config.txt, env_vars, private_config.txt, ni system_env_vars.

PASO 1 En la ventana Administrador de archivos, seleccione la ficha **Archivos**.

PASO 2 En la jerarquía **Sistema de dispositivos/archivo**, navegue hasta la carpeta de la memoria flash que contiene la carpeta o los archivos que desee eliminar.

PASO 3 Marque la casilla de la misma fila que el archivo o carpeta que desee eliminar.

Puede seleccionar más de un archivo o carpeta para eliminar. Cuando se selecciona una carpeta, se eliminarán todos los archivos de esa carpeta y sus subcarpetas.

PASO 4 Haga clic en **Aplicar**.

PASO 5 Si desea eliminar el archivo en forma permanente de un sistema de archivos de clase B, realice una compresión en el sistema de archivos en el que existe dicho archivo.

PASO 6 Realice los siguientes pasos para restaurar un archivo que no se haya eliminado permanentemente por medio de una compresión:

a. Marque la casilla de la misma fila que el archivo que desee restaurar.

b. Haga clic en **Aplicar**.

PASO 7 Realice los siguientes pasos para comprimir un sistema de archivos de clase B:

a. Marque la casilla de la misma fila que el sistema de archivos que desee comprimir.

b. Haga clic en **Aplicar**.

Cuando se comprima un sistema de archivos, si existen archivos en éste que estén marcados para ser restaurados, dichos archivos se restauraran antes que comience la compresión. Los archivos marcados para su eliminacion se eliminan antes de la operación de compresión. Las compresiones pueden tardar varios minutos.

Administración de cargas telefónicas

Para acceder a las opciones de administración de cargas telefónicas, seleccione **Administración** > **Administración de cargas telefónicas**.

- **Visión general**
- **Eliminar cargas telefónicas**
- **Cargar cargas telefónicas**
- **Arrastrar y soltar actualizaciones de teléfonos (teléfonos IP seleccionados de las series SPA500, SPA300, SPA6900 y de la serie 7900)**

Visión general

En las fichas de la ventana Administración de cargas telefónicas, se puede:

- Cambie o agregue cargas de teléfonos en la memoria flash compacta especificando un paquete de software para el UC500. Las cargas telefónicas se extraen del paquete de software y se cargan en el UC500.
- Elimine las cargas telefónicas de la memoria flash compacta del UC500 para optimizar el espacio de la memoria flash.
- Reemplace una carga telefónica específica eliminando la versión que está actualmente en el sisteam y al cargar una versión más nueva.

Para cargar los archivos de cargas telefónicas en el UC500, asegúrese que se haya desactivado cualquier servidor TFTP o FTP de terceros que se ejecuten en la PC que está ejecutando Configuration Assistant.

Eliminar cargas telefónicas

Cuando se selecciona la ficha Eliminar cargas telefónicas, todas las cargas telefónicas del UC500 se muestran en la lista.

- Se muestra una casilla de verificación en la columna Seleccionar para todas las cargas telefónicas disponibles en la memoria flash del UC500.
- Las cargas telefónicas que no están en uso en el sistema se marcan y pueden eliminarse con seguridad.
- Las cargas telefónicas que están en uso no están marcadas.

Para eliminar una carga telefónica, siga estos pasos:

PASO 1 Haga clic en la fila de la tabla para esa carga telefónica para destacarla.

PASO 2 Asegúrese que esté marcada la casilla de verificación de la columna **Seleccionar** para esa carga telefónica.

Haga clic en **Eliminar**.

PASO 3 Repita los pasos anteriores para eliminar cargas telefónicas adicionales.

A medida que elimine cargas telefónicas, los campos **Espacio disponible en flash** se actualizan para reflejar la utilización de la memoria flash después de su eliminación.

PASO 4 Haga clic en **Aceptar** cuando termine de eliminar las cargas telefónicas.

Cargar cargas telefónicas

Para cargar cargas telefónicas en el UC500, siga estos pasos:

PASO 1 Haga clic en **Explorar** y ubique el paquete de software para el UC500 (archivo .ZIP) que contiene las cargas telefónicas que desea cargar, por ejemplo; `UC520-7.0.3.zip` o `UC540-7.1.1.zip`.

Una vez que haya seleccionado el archivo del paquete de software para el UC500, CCA analiza las cargas telefónicas en el paquete de software y las que se usan en su sistema.

Cuando se completa el análisis del paquete de software, se muestra la lista de cargas telefónicas disponible en la imagen especificada. Se selecciiona cargar las cargas telefónicas que ya están en utilización en su sistema.

Haga clic en la casilla de la columna **Seleccionar** para seleccionar o no las cargas telefónicas de la lista de aquellas que van a cargarse.

NOTA Las cargas telefónicas 521_524 para teléfonos CP500 no pueden marcarse como no seleccionadas. Se debe actualizar al último firmware para que estos teléfonos funcionen correctamente.

PASO 2 Haga clic en **Cargar** para cargar las cargas telefónicas seleccionadas en el UC500.

PASO 3 Haga clic en **Aceptar** para cerrar la ventana Administración de cargas telefónicas.

Arrastrar y soltar actualizaciones de teléfonos (teléfonos IP seleccionados de las series SPA500, SPA300, SPA6900 y de la serie 7900)

El método de arrastrar y soltar actualizaciones de cargas de teléfonos puede usarse para actualizar firmware para los siguientes teléfonos IP:

- Teléfonos IP modelos 6901, 6911, 6921, 6941 e 6961 de Cisco (el modelo 6945 no se admite)
- Teléfonos IP de la serie SPA500 de Cisco (incluyendo SAP525G y SPA525G2)
- Teléfonos IP de Cisco serie SPA300
- Teléfonos IP modelos 7975, 7970, 7971, 7945, 7965, 7942, 7962, 7941, 7961, 7931, 7911, y 7906 de Cisco

Estas pautas y notas se aplican a las actualizaciones de cargas de teléfonos de arrastrar y soltar:

- Este método de actualizaciones sólo se admite en los teléfonos indicados anteriormente. CCA muestra un mensaje si no reconoce el formato del archivo de carga de teléfonos.
- Para la mayoría de los teléfonos modelos 79xx de Cisco, no se tiene que extraer los archivos desde un archivo .ZIP. Para los teléfonos de las series SPA500 y SPA300 de Cisco, se debe extraer el archivo .bin del archivo antes de arrastrarlo y soltarlo sobre la topología. Las cargas de teléfonos para los modelos 7921 y 7925 de Cisco están en un paquete de archivos .tar que se puede arrastrar y soltar sobre el icono del UC500.
- No se puede arrastrar y soltar más de un archivo a la vez.
- Las cargas de teléfonos se copian en el directorio `flash:phones/` de la memoria flash del UC500 y se ubican en el subdirectorio adecuado para el modelo del teléfono. Por ejemplo: `flash:phones/525` ó `flash:phones/5x5`.
- Una vez que se descarga el firmware actualizado, puede administrarse por medio de la ventana Administración de carga de teléfonos en CCA.

Para actualizar los teléfonos IP de Cisco que usen el método de arrastrar y soltar, siga estos pasos.

PASO 1 Descargue el software para teléfonos desde Cisco.com, se necesita un inicio de sesión en Cisco.com.

PASO 2 Inicie CCA y conéctese al sitio de clientes o al dispositivo UC500.

PASO 3 Seleccione **Inicio** > **Topología** para abrir la vista Topología, si es que ya no está abierta.

PASO 4 En la PC que ejecuta CCA, ubique el archivo de firmware para telefonos que se descargó desde Cisco.com. Por ejemplo: `spa525g-7-4-3.bin`.

PASO 5 En la vista Topología, use el ratón para arrastrar el archivo de carga de teléfonos (.ZIP o .BIN) desde su PC y suéltelo sobre el icono del UC500.

Si CCA reconoce el archivo como una carga de teléfonos válida, aparece un diálogo emergente y se le solicitará cargar el archivo.

PASO 6 Haga clic en **Cargar**. El diálogo muestra el progreso de carga y actualización.

Una vez que se aplique la actualización, se le solicitará reiniciar todos los teléfonos involucrados.

Para reiniciar un teléfono usando CCA, abra la vista Topología, haga clic con el botón derecho en el icono del teléfono y seleccione **Reiniciar**.

19

Supervisar

Lea esta sección para aprender acerca de los informes e información de diagnóstico que puede monitorearse para los dispositivos en un sitio de clientes. Para acceder a las opciones de monitoreo del sistema, seleccione **Supervisar** en la barra de funciones.

Están disponibles las siguientes categorías de informes y herramientas de monitoreo:

- **Red**
- **Seguridad**
- **Telefonía**
- **Inventario**
- **Estado**
- **Notificación de eventos**
- **Registro del sistema**
- **Mensajes del sistema**
- **Estado de múltiples sitios**

Red

Para acceder a las opciones de monitoreo de estado de red, seleccione **Supervisar** > **Red** en la barra de funciones. Están disponibles las siguientes herramientas e informes de monitoreo:

- **Estadísticas de puertos**
- **Gráficos de ancho de banda**
- **Gráficos de enlaces**
- **Utilización inalámbrica**
- **Estado T1/E1/BRI**
- **DNS y Hosts**

Estadísticas de puertos

Para acceder a las Estadísticas de puertos, seleccione **Supervisar** > **Red** > **Estadísticas de puertos** en la barra de funciones.

Las Estadísticas de puertos están disponibles sólo para los switches de la serie ESW500 y CE520de Cisco.

En la ventana Estadísticas de puertos, se puede mostrar información de los puertos, como estadísticas sobre desempeño de enlaces, paquetes rechazados y errores totales. Para ver una vista condensada y gráfica de las estadísticas del puerto, utilice la ventana **Gráficos de ancho de banda**.

- Para ver estas estadísticas para los puertos en un dispositivo determinado, seleccione el dispositivo de la lista Nombre del host.
- Para actualizar las estadísticas, haga clic en **Actualizar**.
- Para borrar las estadísticas para todos los puertos en el dispositivo seleccionado, haga clic en **Borrar contadores**.
- Para guardar el informe de un dispositivo local, haga clic en **Guardar informe**. En la ventana que aparece, seleccione una carpeta para almacenar el informe.

La siguiente tabla explica los datos de cada una de las fichas: Visión general, Detalle de transmisión y Detalle de recepción.

Ficha	Columna	Explicación
Visión general	Interfaz	Nombre de la interfaz de puertos (por ejemplo, en un switch ESW-540-8P), las interfaces tienen números entre g1 y g9.
	Descripción del puerto	Sólo switches de la serie ESW500. Descripcion para este puerto, si está configurado en el switch.
	Velocidad de transmisión	La velocidad de transmisión actual en Mbps. Incluye la transmisión de paquetes en mal estado y de la retransmisión debido a colisiones en operaciones half-duplex.
	Velocidad de recepción	La velocidad de recepción actual en Mbps. Incluye los bytes de datos de los paquetes en mal estado, paquetes descartados y paquetes sin destino.
	Utilización del ancho de banda para transmisión	El porcentaje de uso de ancho de banda para transmisión, en base a la velocidad de transmisión actual y a la velocidad real.
	Utilización de ancho de banda para recepción	El porcentaje de uso de ancho de banda para recepción, en base a la velocidad de recepción actual y a la velocidad real.
	Velocidad de paquetes de transmisión	La velocidad de transmisión actual de los paquetes bien formados. Incluye paquetes de unidifusión, multidifusión y de difusión.
	Velocidad de paquetes de recepción	La velocidad de recepción actual de los paquetes bien formados. Incluye paquetes de unidifusión, multidifusión y de difusión.
	Velocidad de paquetes de multidifusión/ difusión para transmisión	La velocidad de transmisión actual de los paquetes bien formados de multidifusión y difusión. Excluye a los paquetes de unidifusión.
	Velocidad de paquetes de multidifusión/ difusión para recepción	La velocidad de recepción actual de los paquetes bien formados de multidifusión y difusión. Excluye a los paquetes de unidifusión.
	Total de paquetes descartados	La cantidad total de paquetes descartados tanto desde transmisión como recepción.

Ficha	Columna	Explicación
Visión general	Total de paquetes con error	La cantidad total de paquetes con errores tanto desde transmisión como recepción.

Ficha	Columna	Explicación
Transmitir paquetes	Interfaz	Nombre de la interfaz de puertos (por ejemplo, en un switch ESW-540-8P), las interfaces tienen números entre g1 y g9.
	Descripción del puerto	Sólo switches de la serie ESW500. Descripcion para este puerto, si está configurado en el switch.
	Unidifusión	El número total de paquetes de unidifusión bien formados transmitidos por un puerto. Se excluyen los paquetes transmitidos con errores o con direcciones de destino de difusión o multidifusión.
	Multidifusión	El número total de paquetes de multidifusión bien formados transmitidos por un puerto. Se excluyen los paquetes transmitidos con errores o con direcciones de destino de difusión o unidifusión
	Difusión	El número total de paquetes de difusión bien formados transmitidos por un puerto. Se excluyen los paquetes transmitidos con errores o con direcciones de destino de unidifusión o multidifusión.
	Colisión total	Número total de paquetes transmitidos sin errores después de tener de 1 a 15 colisiones. Incluye paquetes de todos los tipos de direcciones de destino y excluye los paquetes descartados debido a recursos insuficientes o colisiones tardías.
	Colisión excesiva	Número total de paquetes que no fueron transmitidos después de 16 colisiones. Incluye paquetes para todos los tipos de direcciones de destino.
	Colisión tardía	Número total de paquetes descartados debido a colisiones tardías detectadas durante la transmisión. Incluye todos los paquetes transmitidos que tuvieron una colisión después de la transmisión del sexagésimo cuarto byte del paquete. En el conteo de bytes de frame no se incluyen el preámbulo ni el SFD.

Ficha	Columna	Explicación
Recibir paquetes	Interfaz	Nombre de la interfaz de puertos (por ejemplo, en un switch ESW-540-8P), las interfaces tienen números entre g1 y g9.
	Descripción del puerto	Sólo switches de la serie ESW500. Descripcion para este puerto, si está configurado en el switch.
	Unidifusión	El número total de paquetes de unidifusión bien formados recibidos en un puerto. Se excluyen los paquetes recibidos con errores, con direcciones de destino de difusión o multidifusión, o paquetes de tamaño muy pequeño, o muy grandes. Además, se excluyen los paquetes descartados o sin destino.
	Multidifusión	El número total de paquetes de multidifusión bien formados recibidos en un puerto. Se excluyen los paquetes recibidos con errores, con direcciones de destino de difusión o unidifusión, o paquetes de tamaño muy pequeño, o muy grandes. Además, se excluyen los paquetes descartados o sin destino.
	Difusión	El número total de paquetes de difusión bien formados recibidos en un puerto. Se excluyen los paquetes recibidos con errores, con direcciones de destino de unidifusión o multidifusión, o paquetes de tamaño muy pequeño, o muy grandes. Además, se excluyen los paquetes descartados o sin destino.
	Descartados	El número total de paquetes descartados debido al ancho de banda de recepción o al espacio del búfer de recepción insuficientes o porque las normas de envío estipulan que no serán enviados.

Ficha	Columna	Explicación
Recibir paquetes	Errores de alineación	El número total de paquetes recibidos con errores de alineación. Incluye todos los paquetes recibidos tanto con un error de FCS como con un número no entero de bytes.
	Errores de FCS	El número total de paquetes recibidos con errores FCS. Se excluyen paquetes de tamaño muy pequeño con errores FCS.
	Fragmentos de colisión	Número total de tramas menores que 64 bytes que tienen un número entero de bytes y malos valores FCS.
	Paquetes de tamaño muy pequeño	Número total de paquetes recibidos con menos de 64 bytes que tienen valores FCS buenos.
	Paquetes de tamaño muy grande	Número total de paquetes recibidos con más de 1518 bytes que tienen valores FCS buenos.

Gráficos de ancho de banda

En la ventana Gráficos de ancho de banda, se puede visualizar una estimación del tráfico que pasa por el dispositivo que se seleccione en la lista Nombre de host. Los Gráficos de ancho de banda sólo están disponibles para los switches CE520.

Para visualizar un gráfico de ancho de banda para un switch CE520, debe realizar cualquiera de las siguientes acciones:

- Haga clic con el botón derecho en un miembro del sitio en la vista Panel frontal y seleccione Gráficos de ancho de banda en el menú desplegable.
- Haga clic con el botón derecho, o haga doble clic, en un miembro del sitio en la vista Topología y seleccione Gráficos de ancho de banda en el menú desplegable.
- Seleccione un miembro del sitio en cualquiera de las vistas, y seleccione **Supervisar** > **Red** > **Gráficos de ancho de banda** en la barra de funciones.

Visión general

En caso que se seleccione un switch Catalyst Express 500, un gráfico de ancho de banda entrega las siguientes estimaciones:

- Cuánto ancho de banda se está utilizando, comenzando en el momento en que aparece el gráfico
- Cuánto ancho de banda se ha usado en el último minuto, hora, día ó 2 semanas

Procedimientos

La ventana tiene estas fichas:

- **Serie de tiempo**, que muestra el porcentaje de ancho de banda usado, comenzando en el momento en que aparece la ventana.
- **Tendencias**, que muestra el porcentaje de ancho de banda usado en el último minuto, hora, día o últimas dos semanas.

Serie de tiempo

Es posible manipular el gráfico de esta ficha al

- Seleccionar el tipo de gráfico que aparece
- Cambiar los incrementos en el eje x
- Cambiar el intervalo de encuesta
- Avanzar por el eje x

Seleccionar el Tipo de gráfico que aparece

En la lista Tipo, haga clic en Línea o Barra para seleccionar un tipo de gráfico. En un gráfico de línea, los puntos de datos están conectados por una línea. En un grafico de barras, los puntos de datos se indican por la altura de las barras.

Cambio de los incrementos en el eje x

Por defecto, los incrementos de tiempo en el eje x son cada 2 minutos. Para acercar o alejar la vista de éstos, haga clic en los botones Zoom.

Cambio del intervalo de encuesta

En intervalos regulares, Configuration Assistant solicita que los dispositivos administrados reúnan datos de utilización por dispositivo o por enlace. Este intervalo se llama el intervalo de encuesta del gráfico. Para determinarlo, abra la ventana Preferencias, haga clic en la ficha General y seleccione un valor para el campo Intervalo de encuesta del gráfico.

Nota: Cuando el nivel de tráfico caiga en forma marcada en un dispositivo, no se verá un cambio en el gráfico durante, al menos, 15 minutos, sin importar la configuración del intervalo de encuesta del gráfico.

Avance por el eje x

Es posible utilizar la barra de desplazamiento en la parte inferior del gráfico para desplazarse hacia la izquierda y revisar puntos de datos anteriores que se han quedado fuera del gráfico. Entonces, puede desplazarse hacia la derecha para volver a los datos más recientes.

Nota: El gráfico se actualiza cada vez que el dispositivo es encuestado. Puede cambiar el intervalo de encuesta (la frecuencia para recopilar los datos) seleccionando y usando la ventana Preferencias.

Tendencias

El gráfico de esta ficha muestra la utilización del ancho de banda previo. Por lo tanto, podrá visualizar los datos históricos cuando abra esta ficha; por defecto, se trata de los datos del ancho de banda del dispositivo de los últimos 60 segundos. Si se hace clic en los botones tendencia de la ficha, también es posible visualizar los datos de los últimos 60 minutos, 24 horas ó 14 días. Estos datos siempre aparecen como un gráfico de barras. Los intervalos del eje x se determinan para cada gráfico de tendencias; es posible alargarlos o acortarlos sólo hacienco clic en un botón diferente.

Gráficos de enlaces

Los gráficos de enlaces están disponibles sólo para los switches de la serie ESW500 y CE520de Cisco.

Para desplegar un gráfico de enlace, un extremo del enlace debe estar conectado a un puerto en un dispositivo miembro. No es posible desplegar un gráfico de enlace entre los dispositivos candidatos.

Para desplegar un gráfico de enlace, realice cualquiera de las siguientes acciones:

- Seleccione **Supervisar** > **Red** > **Gráficos de enlace** en la barra de funciones.
- Haga clic en la vista de topología y elija **Gráficos de enlace** del menú emergente.

NOTA Usted puede cambiar el intervalo de encuestas del gráfico seleccionando y usando la ventana Preferencias.

Visión general

Un gráfico de enlace muestra:

- El porcentaje de ancho de banda que está siendo utilizado

- La cantidad de bytes transmitidos y recibidos
- La cantidad de paquetes transmitidos y recibidos (diferenciados en paquetes de difusión/multidifusión y paquetes de unidifusión)
- El total de errores y paquetes rechazados

En la ventana Gráficos de enlaces, usted puede:

- **Seleccionar el tipo de datos desplegados**
- **Seleccionar el tipo de gráfico desplegado**
- **Cambiar los incrementos en los ejes**
- **Ver un largo intervalo de datos**

Procedimientos

Para seleccionar un puerto distinto al que aparece en el campo **Interfaz**, sobreescriba el número del puerto, utilice los botones de desplazamiento o haga clic en el icono de selección de puertos. Si elije la última opción, se abre la ventana Seleccionar la interfaz para mostrar el panel frontal del dispositivo. Seleccione el puerto haciendo clic en él; luego haga clic en **Aceptar**. Consulte **Seleccionar la interfaz, página 597**.

Seleccionar el tipo de datos desplegados

Para seleccionar el tipo de datos, haga clic en **% de utilización**, **Paquetes transmitidos/recibidos**, **Métodos de envío de paquetes** o **Errores y rechazos de paquetes** en la lista **Datos**. Los resultados de cada selección se describen en esta tabla:

Tipo de datos	Resultados
% de utilización	Muestra el porcentaje de ancho de banda que está siendo utilizado en el puerto que corresponde al enlace. Por ejemplo, si el ancho de banda del enlace es 100 Mbps, y 20 Mb son consumidos a la vez, el gráfico muestra 20% en ese instante.

Tipo de datos	Resultados
Paquetes transmitidos/ recibidos	Muestra dos gráficos: Transmitido (rojo) y Recibido (azul). El gráfico Bytes transmitidos muestra el número de bytes transmitidos en el puerto que corresponde al enlace. El gráfico Bytes recibidos muestra el número total de bytes recibidos en el puerto que corresponde al enlace.
Métodos de envío de paquetes	Muestra dos gráficos: Paquetes de difusión/ multidifusión (rojo) y Paquetes de unidifusión (azul). El gráfico Paquetes de difusión/multidifusión muestra la cantidad de paquetes de difusión y multidifusión recibidos y transmitidos al puerto que corresponde al enlace. El gráfico Paquetes de unidifusión muestra la cantidad de paquetes de unidifusión recibidos y transmitidos al puerto que corresponde al enlace.
Errores y rechazos de paquetes	Muestra dos gráficos: Total de errores (azul) y Total de paquetes rechazados (rojo). El gráfico Total de errores muestra el número total de paquetes con errores que se han acumulado en el puerto desde la última vez que se restablecieron los contadores. El gráfico Total de paquetes rechazados muestra la cantidad total de paquetes que fueron rechazados en el puerto que corresponde al enlace. Los paquetes son rechazados debido a la falta de búfers o de ancho de banda o debido al filtro de paquetes configurados por el usuario en el dispositivo.

Seleccionar el tipo de gráfico desplegado

De la lista **Tipo**, haga clic en **Línea**, **Barra**, **Barra de apilamiento**, **Área** o **Área de apilamiento** para seleccionar un tipo de gráfico. La apariencia de cada tipo se describe en esta tabla.

Tipo de gráfico	Apariencia
Línea	Los puntos de datos están conectados mediante una línea.
Barra	Los puntos de datos se indican mediante la altura de las barras.
Barras apiladas	Los múltiples gráficos de barra, cada uno de distinto color, se apilan uno sobre otro.
Área	Los puntos de datos están conectados mediante una línea y el área bajo la línea está rellenada.
Áreas apiladas	Los múltiples gráficos de área, cada uno de distinto color, se apilan uno sobre otro.

Cambiar los incrementos en los ejes

Por defecto, los incrementos de tiempo en el eje x son cada 2 minutos. Para acercar o alejar la vista de éstos, haga clic en los botones **Zoom**.

Marque **Escala del registro** si desea que los incrementos en el eje escalen en forma logarítmica más que aritmética.

Ver un largo intervalo de datos

Utilice la barra de desplazamiento en la parte inferior del gráfico para desplazarse hacia la izquierda y revise los puntos de datos anteriores que están fuera del gráfico. Entonces, puede desplazarse hacia la derecha para volver a los datos más recientes.

NOTA El gráfico se actualiza cada vez que el dispositivo es encuestado. Puede cambiar el intervalo de encuesta (la frecuencia para recopilar los datos) en la ventana Preferencias.

Seleccionar la interfaz

Esta ventana aparece cuando usted hace clic en un icono de puerto de switch en una ventana de Configuration Assistant. Muestra el panel frontal de un switch seleccionado. Utilice la ventana para seleccionar una interfaz en el switch.

Siga estos pasos:

PASO 1 Haga clic en la interfaz que desee utilizar.

Las interfaces que no puede seleccionar aparecen en gris.

PASO 2 Haga clic en **Aceptar**. Usted vuelve a la ventana de Configuration Assistant que estaba usando y el nÃºmero de la interfaz seleccionada aparece en el campo Interfaz.

Utilización inalámbrica

Para ver un informe de la utilización inalámbrica, seleccione **Monitorear** > **Red**> **Utilización inalámbrica** en la barra de funciones.

Sólo está disponible la información de estado para clientes inalámbricos para los siguientes dispositivos:

- Plataformas UC500 y routers de la serie SR500 de Cisco con un punto de acceso incorporado
- Puntos de acceso autónomos AP521 de Cisco
- Puntos de acceso de radio única y doble banda AP541N de Cisco

No se muestra el estado del controlador LAN inalámbrica.

Seleccione un dispositivo inalámbrico del menú de la lista Nombre de host.

El informe Utilización inalámbrica muestra la siguiente información para cada cliente conectado:

- Su dirección MAC
- Nombre
- Su dirección IP
- Número de VLAN
- SSID (identificador de sitio seguro)
- Tipo de administración de claves
- Tipo de cifrado
- Velocidad de datos, en Mbps

- Intensidad de la señal, en dBM, para los clientes conectados a puntos de acceso AP521 y UC500 incorporados
- RSSI (indicación de intensidad de señal recibida) para puntos de acceso AP541N

  La RSSI indica la intensidad de la señal de RF (radio frecuencia) para los clientes conectados a puntos de acceso AP541N. Se muestra un valor entre 1 y 100.
- Paquetes que entran/salen
- Bytes que entran/salen

Estado T1/E1/BRI

Si hay una interfaz T1/E1 ó BRI presente el sistema, seleccione **Supervisar** > **Red** > **Estado de T1/E1/BRI** de la barra de funciones para ver la salida de los comandos de IOS de Cisco como **mostrar estado de isdn**y **mostrar controlador**para bri, t1, ó e1, dependiendo de las interfaces disponibles.

DNS y Hosts

Seleccione **DNS y Hosts** para ver la salida del comando **mostrar hosts** para el sitio del cliente. La salida incluye el nombre de host y dominio DNS del UC500 ó SR500 y las direcciones IP de los servidores DNS primarios y secundarios.

Seguridad

Para acceder a las opciones de monitoreo para seguridad de la red, seleccione **Supervisar** > **Seguridad**en la barra de funciones. Los informes de seguridad del modo experto se indican y describen a continuación.

Estos informes se basan en texto y se generan a partir de la salidad de comandos IOS de Cisco.

NOTA Estos reportes principalemente buscan ayudar al Small Business Support Center (SBSC) en la resolución de problemas con las implementaciones de SBCS de Cisco. Se necesita un conocimiento experto de IOS de Cisco y de la interfaz de línea de comandos para interpretar efectivamente los datos presentados en estos informes.

Informe de seguridad	Descripción
Cliente y servidor EZVPN	Muestra la salida de los comandos **mostrar cifrado** para obtener información acerca de las actuales asociaciones de seguridad, la configuración remota de EasyVPN, la configuración que utilizan actualmente las SA, las sesiones VPN activas y las estadísticas del acelerador de cifrado.
Estado de VPN de sitio a sitio	Muestra la salida de los comandos **mostrar cifrado** para obtener las actuales asociaciones de seguridad, la configuración remota de EasyVPN, la configuración que utilizan actualmente las SA, las sesiones VPN activas y las estadísticas del acelerador de cifrado.
Estado de VPN sobre SSL	Muestra la salida de los comandos **mostrar tcp** y **mostrar webvpn** para obtener información acerca de los puntos de extremos de las conexiones TCP, las sessiones de usuarios de VPN sobre SSL y estadísticas del túnel VPN sobre SSL. Para mostrar la información de la sesión de un usuario específico de VPN sobre SSL, especifique el nombre y haga clic en **Consultar**.
Firewall	Muestra la salida de los comandos **mostrar lista de acceso** y **mostrar sesión de inspección de ip**.
NAT	Muestra la salida de los comandos **mostrar nat ip** y **mostrar ruta ip** para obtener información acerca de las estadísitcas de NAT, rutas IP y traducciones NAT.
Estado de la red VPN	Consulte **Estado de la red VPN, página 600**.

Estado de la red VPN

Aparece la ventana de estado de VPN cuando se selecciona **Supervisar** > **Seguridad** > **Estado de VPN** en la barra de funciones.

EasyVPN

En esta ficha, se puede monitorear el estado de los túneles EasyVPN.

Seleccione un dispositivo sobre el cual informar de la lista Nombre de host. Las entradas de informes se pueblan automáticamente.

Estado de la red VPN	Descripción
ACTIVA	Activo y funcionando.
ACTIVA - DETENIDA	Activo, pero no hay actividad.
ACTIVA, SIN IKE	Activo, pero sin IKE (Intercambio de claves por Internet).
INACTIVO, NEGOCIANDO	Inactivo, pero el dispositivo está negociando la conexión.
INACTIVA	Inactivo.

VPN sobre SSL

En esta ficha, se puede monitorear el estado de los túneles VPN sobre SSL (capa de conexión segura).

Telefonía

Para acceder a las opciones de monitoreo para funciones de telefonía, seleccione **Supervisar** > **Telefonía** en la barra de funciones. Los informes de telefonía del modo experto se indican y describen a continuación.

Estos informes se basan en texto y se generan a partir de la salidad de comandos IOS y CUE de Cisco.

NOTA Estos reportes principalemente buscan ayudar al Small Business Support Center (SBSC) en la resolución de problemas con las implementaciones de SBCS de Cisco. Se necesita un conocimiento experto de IOS y CUE de Cisco y de la interfaz de línea de comandos para interpretar efectivamente los datos y la salida presentada en estos informes.

Informe de telefonía	Descripción
Teléfonos y anexos	**Teléfonos**. Muestra el estado e información de sólo lectura de la configuración interna para los teléfonos y anexos, incluyendo la asignación de fichas, direcciones MAC, tipo de teléfono, nombre de usuario y de botones, plantilla telefónica en uso, dirección IP, carga de teléfono que se está usando y estado. **Anexos**. Para cada anexo, se muestra la ficha DN, el número de anexo interno, el tipo de línea, etiqueta, nombre de usuario, COR entrantes, tipo de enlace troncal y estado del canal. Si están configurados, el número y etiqueta del intercomunicador también se muestran. Los números del intercomunicador comienzan con una caracter alfabético (por ejemplo, A502).
Grupos de llamado	Muestra la información de configuración interna para los grupos de llamado, incluyendo la ficha, número piloto, tipo, miembros, configuración de límite de tiempo y destino para Sin respuesta enviar a. **Buscar grupos por miembro**. Especifique un número de anexo o una serie de números separados por una coma para encontrar un grupo o grupos de llamado al que pertenezca un número de anexo.
Grupos de envío de llamadas	Muestra la información de configuración interna para los grupos de llamado, incluyendo la ficha, número piloto, tipo, miembros, configuración de límite de tiempo y destino para Sin respuesta enviar a. **Buscar grupos por miembro**. Especifique un número de anexo o una serie de números separados por una coma para encontrar un grupo o grupos de envío de llamadas al que pertenezca un número de anexo. Seleccione un grupo y haga clic en **Ver resumen de configuración** para mostrar información de resumen de CLI para el grupo de envío de llamadas seleccionado.

Informe de telefonía	Descripción
Archivos del servidor TFTP	Muestra la información del nombre del archivo para los archivos del servidor TFTP almacenados en la memoria flash. Si es aplicable, también se indican el nombre del dispositivo que es dueño del archivo y de su seudónimo.
Pares de discado	Muestra la información de configuración internap para POTS y pares de discado de VoIP configurados en el sistema. **POTS**. Para los pares de discado POTS, la información incluye el número de ficha, descripción de puerto, patrón de destino, destino entrante, nombre de perfil de traducción, valor de dígitos de envío y preferencia de enlace troncal. **VoIP**. Para los pares de discado de VoIP, la información incluye el número de ficha, descripción, patrón de descripción, clase de voz, objetivo de sesión, relé DTMF y códec.
Perfiles de traducción	Muestra la información de configuración interna para los perfiles y normas de traduccion y entrega una opción para las probarlas.
Estado del enlace SIP	Muestra la salida de los comandos **mostrar sip-ua** para el estado del servicio SIP, registro, temporizadores y estadísticas.
Plantilla telefónica	Para la plantilla de teléfono IP seleccionada, se muestran las propiedades de la plantilla interna para las teclas y diseño de botones. Esta información es de sólo lectura; las plantillas no pueden editarse con Configuration Assistant.

Informe de telefonía	Descripción
Estado de correo de voz	Cuando se selecciona un informe de estado de correo de voz, Configuration Assistant muestra un diálogo de Progreso a medida que la conexión al sistema de Correo de voz en el módulo CUE se abre y se recopila la salida de comandos. Están diposnibles informes de estado de correo de voz basados en texto: **Sistema**. Muestra la salida de comandos de mostrar para obtener información acerca de las estadísticas del reloj y zonas horarias, privilegios asignados a los grupos configurados, versiones de software y aplicaciones, licencias compradas para el sistema y paquetes de software instalados. **Correo de voz**. Muestra la salida de los comandos mostrar correo de voz para obtener información acerca de los buzones configurados y su estado de almacenamiento actual, los valores por defecto para todos los buzones y estadísticas de utilización de correo de voz. **Calendario**. Muestra los calendarios y días festivos configurados para el sistema en formato de texto. **Otros**. Muestra la salida de los comandos para obtener información acerca de las aplicaciones configuradas actualmente, los saludos configurados para la contestadora automática, nombres de archivos de comandos y tupos de activaciones configuradas actualmente.
Estado DSP	El informe de estado DSP muestra detalladas salidas de comandos mostrar para el hardware y grupos DSP, errores y DSP activa/señalización de voz.

Informe de telefonía	Descripción
Paquete de software	El informe del Paquete de software muestra el paquete de software y la información de la versión componente, utilización de memoria flash compacta, estado CUE y tipos de teléfonos admitidos para el paquete de software del UC500 instalado actualmente. No está disponible información de versiones de paquetes de software para el UC500 antes de la 7.0.0.
Estado de movilidad de anexos	El informe de estado de movilidad de anexos muestra la información de los teléfonos con movilidad de anexos, la salida del estado de movilidad de anexos, el perfil del teléfono y el del usuario actual. Esta información es sólo de lectura; para configurar estos parámetros, consulte **Movilidad de anexos, página 345**.

Inventario

Para mostrar un informe de inventario para un sitio de cliente o un dispositivo individual, seleccione **Supervisar** > **Inventario**.

El informe de inventario para un sitio de cliente muestra los tipos de dispositivos, números de serie, direcciones IP y versiones de software para el sitio. También se puede seleccionar un solo dispositivo para el que desee ver los detalles de inventario.

La información de esta ventana es de sólo lectura. Para cada dispositivo de la comunidad, el inventario contiene

- Su nombre de host
- Tipo de dispositivo
- Su número de serie
- El número de versión del hardware (ID de versión)
- Su dirección MAC
- Su dirección IP
- La revisión del software instalado

- Ubicación del sistema
- Tiempo activo del sistema (El tiempo durante el cual ha estado funcionando)

Si no se asignó un nombre de host a un switch en el sitio, un nombre de host de **switch-***<número>* se asigna en forma automática. El número muestra el orden en el cual el switch se agregó al sitio.

Haga clic en **Detalles** para ver los detalles de un dispositivo específico. Consulte **Detalles de inventario, página 606**.

Haga clic en **Actualizar** para actualizar la pantalla.

Detalles de inventario

Esta ventana aparece cuando se selecciona un dispositivo con capacidad de enrutamiento y hace clic en **Detalles** en la ventana Inventario.

La ventana muestra información del dispositivo por componente, descripción, número de parte, versión del hardware, número de serie de la tarjeta de circuitos impresos (PCB) y por el número del producto. La descripción entrega los detalles del componente. El número de parte es el número de pedido del componente.

Si usted sabe que ha ocurrido un cambio y desea ver el cambio, haga clic en **Actualizar**. Configuration Assistant vuelve a probar los componentes y vuelve a mostrar los detalles cuando se agregan o eliminan componentes.

Registro del sistema

El informe de Registro del sistema muestra la salida del comando **mostrar registro**.

Estado de múltiples sitios

Se debe conectar directamente a un puerto LAN del router seguro UC520 ó SR520-T1 para ver el estado de múltiples sitios.

El informe de Estado de múltiples sitios muestra la salida del comando **mostrar detalles de sesión de cifrado** de IOS de Cisco. Este comando muestra todas las sesiones activas de la Red privada virtual (VPN) y el IKE (Intercambio de claves por Internet) y SA (asociaciones de seguridad) de IPSec para cada sesión de VPN.

Consulte Monitoreo del estado de múltiples sitios, página 515.

Estado

Es posible monitorear cierta cantidad de mediciones de estado de los dispositivos para evitar las detenciones y asegurar que su red funciona eficientemente. Las mediciones informan acerca de la utilización de banda ancha, PoE (Power over Ethernet), la CPU, y la memoria, y también acerca de la temperatura del dispositivo y el porcentaje de paquetes con errores.

Para revisar las mediciones del estado, seleccione **Monitorear** > **Estado** en la barra de funciones.

Además de las mediciones de estado, Configuration Assistant tiene funciones que se concentran en la utilización de recursos específicos:

- Para obtener información acerca de la utilización de PoE, seleccione **Configurar** > **Puertos** > **Configuración de puertos**.
- Para obtener información acerca de la utilización de banda ancha en el tiempo, seleccione **Supervisar** > **Red** > **Gráficos de banda ancha**.
- Para obtener información acerca de la utilización del enlace, seleccione **Supervisar** > **Red** > **Gráficos de Enlace**.
- Para obtener mayor información acerca de los paquetes con errores, seleccione **Supervisar** > **Red** > **Estadísticas de puerto**.

Utilice la ventana para visualizar los cinco dispositivos que tengan las mediciones más altas en las categorías que ha seleccionado monitorear. Haga clic en las barras de la ventana para mostrar adicionales.

Para obtener incluso mayor información, haga clic en **Detalles** para abrir la ventana Detalles del estado. Consulte Detalles del estado, página 608.

Detalles del estado

Esta ventana aparece cuando hace clic en **Detalles** en la ventana Estado (**Supervisar** > **Estado**). Para una visualización gráfica de esta información, seleccione **Inicio** > **Tablero**.

Cuando termine con esta ventana, haga clic en **Aceptar**.

La ventana Detalles de estado tiene estas fichas:

- **Visión general**
- **Utilización del ancho de banda**
- **Paquetes con errores**
- **Utilización de PoE**
- **Temperatura**
- **Utilización de CPU**
- **Utilización de memoria**

Visión general

La ficha Visión general muestra las mediciones generales de cada una de las categorías que usted monitorea en todos los dispositivos de la red a los que se aplican las categorías. Esta tabla explica las columnas de esta ficha.

Columna	Explicación
Su nombre de host	El nombre de host de un dispositivo autónomo o los nombres de host de los dispositivos de su comunidad.
Utilización del ancho de banda	El promedio de ancho de banda usado para recibir y transmitir paquetes al momento del último intervalo de encuesta.
Paquetes con errores	El porcentaje general (entrada y salida) de paquetes con errores
Utilización de PoE	El porcentaje de voltaje PoE en uso
Temperatura	La temperatura en grados Celsius

Columna	Explicación
Utilización de CPU	El porcentaje de utilización de la CPU en los últimos 5 segundos
Utilización de memoria	El porcentaje de memoria que está siendo usado

Utilización del ancho de banda

La ficha Utilización de ancho de banda muestra el porcentaje de ancho de banda que se está utilizando para recibir paquetes, el porcentaje para transmitir paquetes y el promedio de ambos.

Es posible abrir la ventana Gráficos de ancho de banda para visualizar cómo se está utilizando el ancho de banda en el tiempo. La ventana Gráficos de enlaces mostrará cuáles puertos tienen el mayor tráfico.

Paquetes con errores

La ficha Errores de paquetes muestra el porcentaje de paquetes de entrada y salida del dispositivo que tienen errores y el porcentaje general de errores.

Utilización de PoE

Para los dispositivos que admiten PoE (Power over Ethernet), la ficha Utilización de PoE muestra el porcentaje de voltaje PoE que se está utilizando, el voltaje total, el voltaje utilizado y el disponible. Si se está agregando puntos de acceso y teléfonos IP a su red, conéctelos a dispositivos que muestren una baja utilización de PoE.

Temperatura

Para los dispositivos que pueden medir la temperatura con precisión, la ficha Temperatura muestra, en grados Celsius, la temperatura actual, el umbral de exceso de temperatura y el umbral crítico. Para otros dispositivos, se visualiza que la temperatura está Bien , Normal, con Error, o N/A, indicando que no se detecta la temperatura exacta actual, ni el umbral de exceso de temperatura, ni el umbral crítico.

Utilización de CPU

La ficha Utilización de CPU muestra, por dispositivo, el porentaje de la capacidad de la CPU que se está utilizando en los últimos 5 segundos, en el último minuto y en los últimos 5 minutos.

Utilización de memoria

La ficha Utilización de memoria muestra el porcentaje de memoria que se está utilizando y el número de megabytes totales, libres y usados.

Notificación de eventos

La ventana Notificación de eventos aparece cuando se realiza alguna de estas acciones:

- Hace clic en un icono de eventos o en la barra de estado o en la vista Topología.
- Selecciona **Supervisar** > **Notificaciones de eventos** en la barra de funciones.
- Haga clic en el icono Notificación de eventos de la barra de herramientas.

Visión general

Un evento es una condición que Configuration Assistant detecta y desea que usted conozca. Estos son ejemplos de eventos:

- Alta temperatura en el dispositivo
- Un dispositivo con el ventilador dañado
- Un puerto desactivado en forma administrativa
- Un puerto con una diferencia dúplex
- Un puerto que usted puede configurar con Smartports
- Un dispositivo desconocido en la red
- Conflictos de VLAN

Para que usted sea conciente del evento, Configuration Assistant muestra un mensaje emergente. Además, coloca un icono de evento al que se puede hacer clic en la barra de estado y en la vista Topología, junto al dispositivo en el cual ocurrió el evento. Cuando el puntero del mouse toca un icono de evento en la vista Topología, observará un resumen del evento.

La apariencia del icono depende del tipo de evento. Los tipos de eventos difieren según el número; mientras menor sea el número del tipo, mayor será la necesidad de tomar medidas.

Si Configuration Assistant detecta múltiples eventos, usted verá iconos para todos ellos en la vista Topología. En la barra de estado, usted verá el icono sólo para el evento más urgente.

La ventana Notificación de eventos le entrega una descripción completa de los eventos detectados en la red. Usted usa la ventana para:

- Informar a Configuration Assistant que esté conciente del evento.
- Pedir a Configuration Assistant que tome medidas, en caso de que sea posible.
- Desactivar el LED de Alerta en los switches.

Procedimientos

La ficha Eventos de la ventana de notificación es donde se observan las descripciones de todos los eventos en la red, reconoce su conocimiento de ellos y utiliza Configuration Assistant para resolverlos (en caso de que sea posible)

Para ver un subconjunto de información del evento, haga clic en **Filtro** y utilice la ventana Filtro de notificación. Consulte **Filtro de notificación, página 612**.

Haga clic en **Aceptar** cuando termine en esta ventana.

Esta tabla explica la información sobre la ficha.

Columna	Explicación
Tipo	Indica cuán urgente es resolver el evento. Mientras menor sea el número del tipo, más urgente es la necesidad de resolverlo.
Hora	La hora en que ocurrió el evento.
Descripción de eventos	Una breve descripción de lo ocurrido. Cuando selecciona un evento, aparece una descripción más extensa bajo la lista de eventos.
Capacidad de resolución	**Sí** en caso de que Configuration Assistant pueda resolver el evento, **No** en caso de que no pueda. Usted le pide a Configuration Assistant que resuelva un evento destacándolo y haciendo clic en **Resolver**. Luego, Configuration Assistant abre una ventana para resolver el evento.

Columna	Explicación
Reconocido	Casillas que usted marca para mostrar que esté conciente de los eventos. Si hace clic en **Reconocer todos**, usted reconoce todos los eventos de una vez. Cuando se reconoce un evento, el icono del evento se oscurece.
Dispositivo	El dispositivo involucrado en el evento.

Filtro de notificación

Esta ventana aparece cuando usted hace clic en **Filtrar** en la ventana Notificación de eventos. Utilícela para limitar los tipos de eventos que aparecen en dicha ventana.

Siga estos pasos:

PASO 1 Bajo la opción **Tipos**, desmarque las casillas para los tipos de eventos que se filtrarán. Los eventos de estos tipos no aparecerán en la ventana Notificación de eventos.

PASO 2 Haga clic en **Definir valor por defecto** si cualquiera de las casillas está desmarcada y desea que todas las casillas vuelvan a estar marcadas.

Haga clic en **Aceptar** cuando termine con esta ventana.

Mensajes del sistema

En la ventana Mensajes del sistema se puede ver los mensajes emitidos por los dispositivos de un sitio de clientes.

Para acceder a la ventana Mensaje del sistema, seleccione **Monitorear** > **Mensaje del sistema** en la barra de funciones.

Procedimientos

Siga estos pasos para ver y filtrar mensajes del sistema.

PASO 1 En la lista Nombre de host, seleccione un dispositivo cuyos mensajes desea ver o seleccione **Todos los dispositivos** para ver los mensajes que emiten todos los dispositivos en la comunidad.

PASO 2 Haga clic en el encabezado de una columna de la tabla para ordenar los mensajes de acuerdo a su interés. Por defecto, los mensajes se ordenan por gravedad.

PASO 3 Para ver detalles acerca de un mensaje específico, seleccione su fila en la tabla. Los detalles del mensaje aparecen en el área bajo la tabla.

PASO 4 *Opcional*: Haga clic en **Filtro** para abrir la ventana Filtro de mensajes del sistema, donde puede especificar criterios para limitar los mensajes que aparecen. Consulte **Filtro de mensajes del sistema, página 613**.

PASO 5 *Opcional*: Haga clic en **Guardar informe** para guardar los contenidos de la ventana en un archivo en formato separado por comas. El nombre de archivo por defecto tiene una marca horaria para hacerlo único.

PASO 6 Haga clic en **Aceptar** cuando termine con esta ventana.

Filtro de mensajes del sistema

Esta ventana aparece cuando usted hace clic en **Filtro** en la ventana Mensajes del sistema. Utilícela para limitar los mensajes que aparecen en esa ventana.

Para filtrar los mensajes del sistema, siga estos pasos.

PASO 1 En **Niveles de gravedad**, desmarque las casillas para los niveles de gravedad que se deben filtrar. Los mensajes con estos niveles de gravedad no aparecerán en la ventana Mensajes del sistema.

PASO 2 Haga clic en **Definir valor por defecto** si cualquiera de las casillas está desmarcada y desea que todas las casillas vuelvan a estar marcadas.

Haga clic en **Aceptar** cuando termine con esta ventana.

20

Solución de problemas

Configuration Assistant entrega varias herramientas para solucionar problemas de su sistema:

- **Diagnóstico de circuitos (Retrobucle T1)**
- **Diagnóstico de red**
- **Diagnóstico de telefonía**
- **Diagnóstico de conectividad de CUE**
- **Diagnóstico de seguridad**
- **Depuraciones genéricas**
- **Comandos ejecutables de IOS**
- **Comandos ejecutables de CUE**
- **Generación de un registro de soluciones de problemas del sistema**
- **Enlaces y Conectividad (switches CE520)**

Diagnóstico de circuitos (Retrobucle T1)

Para acceder a la herramienta de diagnóstico del Retrobucle T1 para solucionar problemas del circuito T1, seleccione **Solución de problemas** > **Diagnóstico del circuito** > **Retrobucle T1**.

Este diagnóstico sólo está disponible en un UC500 con una interfaz de voz T1 ó un router SR520-T1 con una conexión WAN de T1.

Visión general

Utilice el diagnóstico del Retrobucle T1 para realizar una prueba de retrobucle local o remoto en un circuito T1.

En las plataformas UC500 con una interfaz T1, también se puede realizar una Prueba de velocidad de error de bit (BERT). Para iniciar una BERT, la conexión T1 debe estar activa y debe estar presente un bucle de extremo lejano en el circuito. Si no lo está, las opciones de BERT no están disponibles.

Durante la operación normal, el campo Errores de BERT (último) debe permanecer en 0. Si se observan errores de velocidad de bits, comuníquese con su proveedor de servicio o empresa de Telecomunicaciones que entrega el circuito T1.

El diagnóstico BERT no está disponible para las plataformas SR520-T1.

Procedimientos

Para realizar un diagnóstico de retrobucle, siga estos pasos:

PASO 1 Seleccione un host de la lista Nombre de host.

PASO 2 Seleccione la interfaz T1. En la mayoría de los casos, sólo se indica una interfaz.

PASO 3 Seleccione un **Tipo de retrobucle** de la lista desplegable.

Los tipos de retrobucle disponibles, dependiendo de si se está ejecutando el diagnóstico en una plataforma UC500 ó en un router seguro SR520-T1 y si está configurado un tipo FDL (Enlace de datos de facilidad).

En el UC500, están disponibles estos tipos de retrobucles:

- Diag
- Línea local
- Carga útil local
- IBOC remoto
- Línea ESF remota (si es Tipo de FDL está configurado como ansi, att o ambas)
- Carga útil remota (si es Tipo de FDL está configurado como ansi, att o ambas)

En la SR520-T, se admiten los siguientes tipos de retrobucles:

- Local
- Remoto
- Carga útil

PASO 4 Opcionalmente, seleccione un Tipo de FDL. Los tipos disponibles son **ansi (ANSI T1.403)**, **att (AT&T TR54016)**, **ambas**, or **ninguno**.

La configuración de Tipo de FDL activa las capacidades adicionales de prueba de bucle remoto enviando información de señalización fuera de banda entre los sitios conectados sobre un circuito T1.

PASO 5 Haga clic en **Bucle activo** para crear el retrobucle en el circuito.

El mensaje **Resumen** desplegado sobre la ventana de salida indica el estado del bucle (conectado en el extremo local, conectado en el extremo remoto, o sin conexión detectada).

se puede hacer clic en **Borrar contadores** para llevar a cero y restablecer los contadores de prueba.

PASO 6 Para iniciar una BERT mientras el bucle está actiuvo, siga estos pasos:

a. Seleccione un patrón. Las opciones disponibles son **Todos en 0**, **Todos en 1**, **2^11-1**, **Alternancia de 0 y 1**, **2^20 QRSS**, **0.151**, y **2^15-1 QRW**.

b. Configure el intervalo de pruebas, desde 1 hasta 14400 minutos.

c. Haga clic en **Iniciar prueba BERT**.

d. Haga clic en **Abortar prueba BERT actual** para detener la prueba.

Haga clic en **Actualizar** para actualizar la interfaz y datos de la prueba BERT.

Los datos de BERT, cuando están presentes, siempre se muestran en la parte superior de la ventana de salida. Los datos de BERT permanecen en la ventana de salida hastga que se hace clic en **Borrar contadores**.

PASO 7 Haga clic en **Bucle inactivo** para quitar el bucle.

Si el bucle aún está activo cuando se cierra esta ventana, se le pedirá quitar todo bucle existente. Se debe quitar los bucles, a menos que se necesite dejarlos activos para una prueba extendida.

Diagnóstico de red

Configuration Assistant entrega varias herramientas de diagnóstico:

- **Hacer ping**
- **Rastreo**
- **Asociaciones DHCP**
- **Estado del sistema**
- **Registro de depuración de WAN (SR520-T1)**

Hacer ping

Para acceder al diagnóstico por Ping, seleccione **Solución de problemas** > **Diagnóstico de red** > **Ping** en la barra de funciones.

El diagnóstico por ping es un método muy común para solucionar problemas de accesibilidad de los dispositivos.

Visión general

Utiliza una serie de mensajes de eco ICMP (Protocolo de mensajes de control) para determinar:

- Si un host remoto está activo o inactivo
- El retraso ida y vuelta en la comunicación con el host
- Pérdida de paquetes

El diagnóstico por ping primero envía un paquete de solicitud de eco a una dirección y espera una respuesta. La prueba de ping tiene éxito sólo si:

- La solicitud de eco llega a destino, y
- El destino puede devolver una respuesta de eco a la fuente dentro de un plazo determinado (llamado límite de tiempo). El valor por defecto para este límite de tiempo es de dos segundos en los routers de Cisco.

Procedimientos

Para realizar una prueba de ping, siga estos pasos:

PASO 1 Seleccione una interfaz de origen (la interfaz WAN por defecto o una interfaz interna/dirección IP).

Para probar la conectividad VPN de sitio a sitio, seleccione una interfaz interna como una VLAN1.

PASO 2 Especifique una dirección IP o nombre de host de destino.

PASO 3 Haga clic en **Ir**.

La salida del comando de ping indica si la prueba tuvo éxito (> 50% de los paquetes transmitidos) y el promedio, mínimo y máximo de los tiempos de ida y vuelta.

Rastreo

Para acceder al diagnóstico de Rastreo seleccione **Solución de problemas** > **Diagnóstico de red** > **Rastreo** en la barra de funciones.

Visión general

El diagnóstico de Rastreo (basado en el comando ruta de trazado de IOS de Cisco) permite determinar la ruta que toma un paquete para llegar a un destino desde un origen determinado al devolver la secuencia de saltos que el paquete ha recorrido.

El rastreo termina cuando:

- El destino responde
- Se supera el máximo de conteos TTL (tiempo de vida)
- Se alcanza en máximo número de saltos (30)
- Se cancela el rastreo

Los resultados del rastreo se muestran en una tabla. La salida paa cada salto muestra el contador de saltos, la dirección IP y el nombre de host asociado con ese salto y la latencia promedio en milisegundos.

Procedimientos

Para ejecutar un diagnóstico de rastreo:

PASO 1 Especifique la dirección IP o nombre de host de destino.

PASO 2 Haga clic en **Ir**.

Asociaciones DHCP

Para acceder al diagnóstico de DHCP seleccione **Solución de problemas** > **Diagnóstico de red** > **Asociaciones DHCP** en la barra de funciones.

El diagnóstico de Asociaciones DHCP muestra las direcciones IP asignadas dinámicamente en el sistema.

No se puede borrar las asociaciones manuales. Sólo se puede borrar las asociaciones automáticas.

La salida muestra la dirección IP, la dirección de hardware (dirección MAC) y la fecha/hora de vencimiento.

Procedimientos

PASO 1 Seleccione una de las siguientes opciones:

- Haga clic en **Liberar asociación seleccionada** para borrar la asociación DHCP seleccionada.
- Haga clic en **Liberar todas las asociaciones** para borrar todas las asociaciones DHCP.
- Haga clic en **Leer asociaciones** para actualizar la lista.

PASO 2 Haga clic en **Aceptar** para cerrar la ventana.

Estado del sistema

Para ver el estado del sistema, seleccione **Solución de problemas** > **Diagnóstico de red** > **Estado del sistema** en la barra de funciones. Esta información también puede verse en la ventana Estado del sistema en el Tablero (**Inicio** > **Tablero**).

La ventana Estado del sistema muestra esta información para los dispositivos administrados en el sitio del cliente:

- Su nombre de host
- Tipo de dispositivo
- Dirección IP de WAN
- Máscara de subred
- Gateway
- Direcciones IP del servidor DNS
- Versión de IOS de Cisco
- Tiempo activo (tiempo transcurrido desde el último restablecimiento del sistema)
- Marca horaria de la última actualización

Registro de depuración de WAN (SR520-T1)

Aparece la pantalla Registro de depuración de WAN cuando está presente el router seguro SR520-T1 en el sitio del cliente y se selecciona **Solución de problemas** > **Diagnóstico de red** > **Registro de depuración de WAN** en la barra de funciones.

Visión general

La función Registro de depuración de WAN permite capturar información de depuración de IOS de Cisco mientras se solucionan problemas en la conexión WAN T1 para el router serguro SR520-T1. También se puede utilizar esta herramienta para obtener la configuración WAN de SR520-T1 y datos del estado de la conexión. La información se recopila en archivos de registro de texto y se guarda en un archivo .ZIP. La facilidad de depuración de IOS de Cisco y los comandos mostrar se utilizan para reunir la información.

PRECAUCIÓN La activación de la recopilación de información de depuración de WAN es intensiva en cuanto a recursos y puede degradar el rendimiento en forma importante. Sólo active la depuración de WAN por periodos breves y evite los periodos de alta utilización, si es posible.

Por este motivo, toda la depuración de WAN se desactiva cuando se cierra la ventana Registro de depuración de WAN o se cierra Configuration Assistant. Si Configuration Assistant se cierra en forma inesperada, estará desactivada la depuración de WAN la próxima vez que se inicie Configuration Assistant.

Procedimientos

Para generar un registro sólo de la salida del comando **mostrar**:

PASO 1 En la ventana Registro de depuración de WAN, haga clic en **Explorar** y seleccione un directorio de archivos de registro.

PASO 2 Haga clic en **Generar registro de solución de problemas**.

No es necesario seleccionar ninguna opción de depuración de WAN ni activar la depuración.

Se crea un archivo de registro de texto en el directorio especificado; no se crea un archivo .ZIP. Este registro incluye el resultado de los comandos mostrar relacionados con la depuración de WAN. Una barra de progreso aparece mientras se genera el registro.

PASO 3 Haga clic en **Aceptar** para cerrar la ventana cuando termine de generar el registro.

Para activar la depuración y recopilar los datos de salida de comandos mostrar y depuración de WAN, siga estos pasos.

PASO 1 En la ventana Registro de depuración de WAN, haga clic en **Explorar** y seleccione un directorio de archivos de registro.

PASO 2 Marque la casilla **T1** para recopilar la información de depuración de WAN T1.

PASO 3 Haga clic en **Aplicar depuración** para activar la depuración.

PASO 4 Reproduzca el problema en su red.

PASO 5 Haga clic en **Generar registro de solución de problemas**.

Se crea un archivo .ZIP en el directorio de archivos de registro especificado. Este registro incluye el resultado de los comandos mostrar relacionados con la depuración de WAN y todos los datos de depuración de WAN. Una barra de progreso aparece mientras se genera el registro.

PASO 6 Haga clic en **Aceptar** para cerrar la ventana cuando termine de generar el registro.

PASO 7 Desactive (desmarque) la depuración de WAN y haga clic en **Aceptar** para cerrar la ventana.

Toda la depuración de WAN se desactiva automáticamente cuando se cierra la ventana.

Diagnóstico de telefonía

Configuration Assistant entrega estas herramientas de diagnóstico de voz:

- **Prueba del plan de numeración**
- **Registro de enlaces SIP**
- **Registro de solución de problemas de voz**
- **Registro de depuración de teléfonos**
- **Captura de PCM**
- **Teléfonos analógicos SCCP**

Prueba del plan de numeración

Para acceder al diagnóstico de DHCP seleccione **Solución de problemas** > **Diagnóstico de telefonía** > **Prueba del plan de numeración** en la barra de funciones.

Utilice la herramienta de diagnóstico Prueba del plan de numeración para ver cómo el plan de numeración enruta las llamadas entrantes y salientes hacia y desde el puerto o anexo especificado en el sistema. Se puede realizar dos tipos de pruebas del plan de numeración:

- **Prueba del plan de numeración saliente**

- **Prueba del plan de numeración entrante**

NOTA Las pruebas del plan de numeración no involucran llamadas activas.

Prueba del plan de numeración saliente

La prueba del plan de numeración saliente muestra cómo se administran las llamadas salientes por parte del plan de numeración saliente.

La prueba verifica los permisos para el anexo de origen (línea compartida o de usuario), las traducciones del número de destino y las posibles rutas (las interfaces salientes en el router) para la llamada.

Dados un anexo de usario y un número de destino, la configuración de voz en el router se examina y se muestran los siguientes datos de llamadas:

- Si se admite la llamada
- El número real enviado al destino
- Todas las potenciales interfaces, junto con sus preferencias
- Las intgerfaces salientes mostradas en la salida de la prueba incluyen los enlaces SIP, si es que están configuradas.
- Para un enlace SIP, se muestra la IP del servidor SIP.

Para realizar una prueba del plan de numeración saliente, siga estos pasos.

PASO 1 Haga clic en la ficha Saliente en la ventana Prueba del plan de numeración.

PASO 2 Seleccione un **Anexo de usuario/compartido** de la lista desplegable.

PASO 3 Especifique el número de destino para la llamada saliente.

El número de destino puede ser un número de anexo interno o un número externo (local, larga distancia o internacional). Puede tener hasta 20 dígitos.

Para los números externos, el número especificado debe incluir todos los códigos de acceso necesarios, tales como el código de acceso PSTN, códigos de acceso de larga distancia, código de área, código de país (por ejemplo 011) ó un código de discado internacional.

PASO 4 Haga clic en **Ver detalles del plan de numeración**.

Prueba del plan de numeración entrante

Para las llamadas entrantes, dados un puerto FXO analógico o un número DID, la prueba del plan de numeración entrante muestra cómo se rutea la llamada y la información básica acerca del anexo de destino.

La salida indica si se encontró un destino coincidente y muestra el número de anexo de destino y tipo de anexo (por ejemplo, usuario, teléfono analógico.

Para realizar una prueba del plan de numeración entrante, siga estos pasos.

PASO 1 Haga clic en la ficha Entrante en la ventana Prueba del plan de numeración.

PASO 2 Seleccione **Puerto FXO analógico** o especifique un **Número DID** para la llamada enrante. El número DID es típicamente un número de formato E.164, por ejemplo, 16905552222.

PASO 3 Haga clic en **Encontrar destino**.

Registro de enlaces SIP

La ventana Registro de enlaces SIP muestra la información de registro SIP y entrega herramientas de diagnóstico para la solución de problemas en el registro de enlaces SIP. Cuando hay un fallo en el registro del enlace SIP, el sistema de voz está desactivado y no pueden hacer ni recibir llamadas por el enlace. Para acceder a esta ventana, seleccione **Solución de problemas** > **Diagnóstico de telefonía** > **Registro de enlaces SIP**.

Para obtener más información, consulte estos temas:

- **Registro de información SIP**
- **Diagnóstico de registro SIP (Registro de ping, Proxy de ping, Registro de restablecimiento)**

Registro de información SIP

Se muestra la siguiente información de registro SIP:

- Si está activo el enlace SIP o no
- Nombre del proveedor del enlace SIP configurado en la ventana Enlace SIP. Puede ser uno de los proveedores que CCA admite o el proveedor de enlace SIP genérico.

- Modelo de registro sIP usado para el proveedor de enlace SIP seleccionado. El modelo de registro puede ser uno de los siguientes:
  - El proveedor de servicios registra el número principal para la ID de quien llama saliente.
  - El proveedor de servicio registra todas las DID utilizando el mismo nombre de usuario y contraseña.
  - El proveedor de servicios registra las DID utilizando diferentes nombres de usuarios y contraseñas. Las credenciales del usuario para cada DID se especifican en **Configurar** > **Telefonía** > **Enlaces** > **Enlace SIP**.
  - El proveedor de servicios no registra las DID (no se necesita registro).
- La dirección IP o nombre de host del servidor de registro SIP, si se configura en la ventana Enlaces SIP.
- La dirección IP o nombre de host del servidor proxy SIP de salida, si se configura en la ventana Enlaces SIP.

Diagnóstico de registro SIP (Registro de ping, Proxy de ping, Registro de restablecimiento)

Se entrega el diagnóstico del registro SIP.

Diagnóstico SIP	Descripción
Registro de ping	Haga clic en **Registro de ping** para verificar la conectividad con el servidor de Registro de SIP que esté configurado en la ventana Enlaces SIP. Dependiendo del resultado obtenido en la prueba de ping, ello podría indicar un fallo en la resolución del nombre del host de DNS, problemas con la configuración de la red, problemas con el firewall o con las ACL que eviten que el tráfico llegue al servidor o un host inubicable.
Proxy de ping	Haga clic en **Proxy de ping** para verificar la conectividad con el servidor de Registro de SIP de salica configurado en la ventana Enlaces SIP.

Diagnóstico SIP	Descripción
Registro de restablecimiento	Cuando se hace clic en **Registro de restablecimiento**, se toman las siguientes acciones: ▪ CCA reconfigura y restablecimiento el servidor de registro SIP. Cuando se restablece el servidor de registro, los temporizadores y contadores de reintentos para el Agente de usuario SIP en Cisco Unified CME. Esto también permite que el registro SIP se reinicie sin el restablecimiento del UC500. ▪ Si se especifica un nombre de dominio para el servidor de registro SIP, CCA reconfigura el grupo fuente de voz interno y las ACL para el firewall CBAC del UC500. Esto puede resolver problemas que se producen si la dirección IP para el servidor de registro se agrega a las ACL al momento de la configuración es diferente a la dirección IP del mismo servidor al momento del registro. Una vez que se restablezca el servidor de registro y se permita un tiempo para el registro con el proveedor de servicio, se puede verificar el estado del registro SIP al ir a la ventana Estado de enlaces SIP (**Monitorear** > **Telefonía** > **Estado de enlaces SIP**). La situación registrada en el panel SIP Registro de la ventana debe mostrar "sí " si el troncal SIP ha registrado con éxito. El enlace SIP intenta registrarse de inmediato. Sin embargo, dependiendo del proveedor, puede tardar varias horas para que las llamadas comiencen a transitar de nuevo una vez que el enlace SIP se haya registrado con éxito.

Registro de solución de problemas de voz

La función de registro de Solución de problemas de voz permite capturar la información de depuración de IOS de Cisco mientras se soluciona un problema o escenario específico. También se puede utilizar esta herramienta para recopilar los datos de configuración de dispositivos relacionados con voz y los del estado de voz. La información se recopila en archivos de registro de texto y se guarda en un archivo .ZIP.

Visión general

La facilidad de depuración de IOS y los comandos mostrar se utilizan para reunir la información. Se puede especificar uno o más de estos tipos de datos de depuración de voz para recopilarlos:

- Plan de numeración
- Puertos de voz
- Teléfonos IP (SCCP)
- VoIP (SIP)
- VoIP (H323)

PRECAUCIÓN La activación de la recopilación de información de depuración de voz es intensiva en cuanto a recursos y puede degradar el rendimiento en forma importante. Sólo active la depuración de voz por periodos breves y evite los periodos de alta utilización, si es posible.

Por este motivo, se desactiva toda la depuración de voz cuando se cierra la ventana Registro de solución de problemas de voz. Si Configuration Assistant se cierra en forma inesperada, estará desactivada la depuración de voz la próxima vez que se inicie Configuration Assistant.

Procedimientos

Para generar un registro sólo de la salida del comando mostrar:

PASO 1 En la ventana Registro de solución de problemas de voz, haga clic en **Explorar** y seleccione un directorio de archivos de registro.

PASO 2 Haga clic en **Generar registro de solución de problemas**.

No es necesario seleccionar ninguna opción de depuración de voz ni activar la depuración.

Se crea un archivo de registro de texto en el directorio especificado; no se crea un archivo .ZIP. Este registro incluye la salida de los comandos mostrar relacionados con la depuración de voz. Una barra de progreso aparece mientras se genera el registro.

PASO 3 Haga clic en **Aceptar** para cerrar la ventana cuando termine de generar el registro.

Para activar la depuración y recopilar los datos del resultado de comandos mostrar y depuración de voz:.

PASO 1 En la ventana Registro de solución de problemas de voz, haga clic en **Explorar** y seleccione un directorio de archivos de registro.

PASO 2 Seleccione uno o más tipos de datos de depuración de voz para recopilarlos.

PASO 3 Haga clic en **Aplicar depuración** para comenzar a general la inforación de la depuración.

PASO 4 Reproduzca el problema en su red.

PASO 5 Haga clic en **Generar registro de solución de problemas**.

Se crea un archivo .ZIP en el directorio de archivos de registro especificado. Este registro incluye el resultado de los comandos mostrar relacionados con la depuración de voz y todos los datos de depuración de voz. Una barra de progreso aparece mientras se genera el registro.

PASO 6 Haga clic en **Aceptar** para cerrar la ventana cuando termine de generar el registro.

PASO 7 Desactive (desmarque) la depuración de voz y haga clic en **Aceptar** para cerrar la ventana.

Toda la depuración de voz se desactiva automáticamente cuando se cierra la ventana.

Registro de depuración de teléfonos

Aparece la ventana Registro de depuración de teléfonos cuando se selecciona **Solución de problemas** > **Telefonía Diagnóstico** > **Registro de depuración de teléfonos**.

Visión general

La función Registro de depuración de teléfonos permite capturar la información de depuración de IOS de Cisco mientras se soluciona un problema o escenario en un teléfono o grupo de teléfonos específico.

También se puede utilizar esta herramienta para recopilar los datos de configuración de dispositivos relacionados con voz y los del estado de voz para el o los teléfonos seleccionados. La información se recopila en archivos de registro de texto y se guarda en un archivo .ZIP.

PRECAUCIÓN La facilidad de depuración de IOS de Cisco y los comandos mostrar se utilizan para reunir la información. La activación de la recopilación de información de depuración de teléfonos es intensiva en cuanto a recursos y puede degradar el rendimiento en forma importante. Sólo active la depuración de teléfonos por periodos breves y evite los periodos de alta utilización, si es posible.

Por este motivo, se desactiva toda la depuración de teléfonos cuando se cierra la ventana Registro de depuración de teléfonos. Si Configuration Assistant se cierra en forma inesperada, estará desactivada la depuración de voz la próxima vez que se inicie Configuration Assistant.

Procedimientos

Para generar un registro sólo de la salida del comando mostrar:

PASO 1 En la ventana Registro de depuración de teléfonos, haga clic en **Explorar** y seleccione un directorio de archivos de registro.

PASO 2 Haga clic en **Generar registro de solución de problemas**.

No es necesario seleccionar ningún teléfono ni activar la depuración.

Se crea un archivo de registro de texto en el directorio especificado; no se crea un archivo .ZIP. Este registro incluye la salida de los comandos mostrar relacionados con la depuración de voz. Una barra de progreso aparece mientras se genera el registro.

PASO 3 Haga clic en **Aceptar** para cerrar la ventana cuando termine de generar el registro.

Para activar la depuración y recopilar los datos del resultado de comandos mostrar y depuración de voz:.

PASO 1 En la ventana Registro de depuración de teléfonos, marque la opción **Activar** para cada teléfono que desee incluir en el registro de depuración. Esta acción

PASO 2 Haga clic en **Explorar** y seleccione un directorio de archivo de registro.

PASO 3 Seleccione uno o más tipos de datos de depuración de voz para recopilarlos.

PASO 4 Haga clic en **Aplicar depuración** para comenzar a general la inforación de la depuración.

PASO 5 Reproduzca el problema en su red.

PASO 6 Haga clic en **Generar registro de solución de problemas**.

Se crea un archivo .ZIP en el directorio de archivos de registro especificado. Este registro incluye el resultado de los comandos mostrar relacionados con la depuración de voz y todos los datos de depuración de voz. Una barra de progreso aparece mientras se genera el registro.

PASO 7 Cuando se genere el registro, apague (desconecte) la depuración para todos los teléfonos y haga clic en **Aceptar** para cerrar la ventana.

Toda la depuración de teléfonos se desactiva automáticamente cuando se cierra la ventana.

Captura de PCM

Aparece la ventana Captura de PCM cuando se selecciona **Solución de problemas** > **Telefonía Diagnóstico** > **Captura de PCM**.

En esta ventana, se puede solucionar problemas de calidad de voz o audioo al generar una captura de PCM (Modulación de código de pulsos) para un puerto de voz específico, según lo indica Soporte de Cisco.

Siga estos pasos para reproducir el escencario de llamada con problemas.

PASO 1 Asegúrese que exista suficiente espacio en la memoria flash del UC500 para crear la captura de PCM. Para hacerlo, seleccione **Inicio** > **Tablero** y mire en la ventana Uso de flash.

PASO 2 Trate de reproducir el escenario de llamadas con problemas.

PASO 3 Una vez que se haya configurado la llamada, examine la salida en los paneles **Tabla de llamadas activas** y **Resumen del estado de llamadas al puerto de voz** para determinar el puerto de voz para la captura de PCM, según lo indica Soporte de Cisco.

La Tabla de llamadas activas muestra la salida del comando **mostrar resumen de voz de llamadas activas** , y el Resumen del estado de llamadas al puerto de voz muestra la salida del **mostrar resumen llamadas de voz**.

Por ejemplo, si la salida de la Tabla de llamadas activas muestra lo siguiente para la configuración de llamdas entre el anexo 201 y el anexo 209 y el anexo 201 está experimentando un problema, entonces el puerto de voz 50/0/10 debería usarse para la captura de PCM.

```
1227 : 26 1118849120ms.1 +2710 pid:20006 Respuesta 201 activo
dur 00:00:06 tx:131/31280 rx:130/31200
Tele 50/0/10 (26) [50/0/10.0] tx:2620/2620/0ms g711ulaw
noise:0 acom:0 i/0:0/0 dBm
```

```
1227 : 27 1118849600ms.1 +2220 pid:20034 Origina 209 activo
dur 00:00:06 tx:130/31200 rx:130/31200
Tele 50/0/18 (27) [50/0/18,0] tx:2600/2600/0ms g711ulaw
noise:0 acom:0 i/0:0/0 dBm
```

PASO 4 En la campo **Puerto de voz**, especifique el identificador del puerto en el que realizar la captura (por ejemplo, 50/0/10.

PASO 5 Haga clic en **Comenzar**.

Cuando se hace clic en **Comenzar**:

- CCA emite estos comando para determinar el búfer de captura y especificar el archivo de destino para la captura (el archivo pcm.dat en la memoria flash del UC500).

  ```
  voice hpi capture buffer 5000000
  voice hpi capture destination flash:pcm.dat
  ```

- El sistema comienza a escribior los datos de PCM al archivo pcm.dat en la memoria flash del UC500.

PASO 6 Cuando esté listo para detener la captura, haga clic en **Terminar y guardar**.

PASO 7 Guarde el archivo de captura pcm.dat.

Después de grabar el archivo, éste se elimina de la memoria flash. El tamaño del archivo de captura varía, dependiendo de las acciones realizadas en la llamada.

Teléfonos analógicos SCCP

Aparece la ventana Teléfono analógico SCCP cuando se selecciona **Solución de problemas**> **Diagnóstico de telefonía** > **Teléfonos analógicos SCCP**.

Los códigos de acceso a funciones permiten que los usuarios de teléfonos analógicos controlados por SCCP puedan acceder a ciertas funciones del teléfono al marcar dócidos (por ejemplo, **1 para configurar Desvíar todas en el teléfono).

Cuando el dispositivo UC500 está con la configuración por defecto de fábrica, el proceso de inicialización de voz elimina el comando de código de acceso de la función stcapp.

En esta ventana se puede activar o desactivar los códigos de acceso de funciones stcapp.

- Cuando **Activar códigos de acceso de funciones stcapp** no está marcado, los códigos de acceso de funciones se configuran por medio de los comandos `fac` en sólo `servicio de telefonía`. Ésta es la configuración recomendada.
- Cuando se marca **Activar códigos de acceso de funciones stcapp**, el comando `códigos de acceso de funciones stcapp` se configura además de los comandos `fac` en servicio de telefonía. Sin embargo, si se activa esta configuración se generan conflictos entre los códigos de funciones, ya que 5, 6, 7 y 8 se configuran en forma diferentes con estos comandos. La salida de los siguientes comandos ilustran el conflicto.

```
UC_540# mostrar códigos de funciones

código de acceso de funciones stcapp
  ID de llamada maliciosa (MCID) ***
  prefijo **
  desviar todas **1
  cancelar desvío **2
  grupo local de contestación **3
  grupo diferente de contestación **4
  meetme-conference **5
  contestación directa **6
```

```
  desvío a correo de voz **7
  cancelar llamada en espera **8

UC540# sh telephony-service fac

  servicio de telefonía fac estándar
  callfwd all **1
  callfwd cancel **2
  grupo local de contestación **3
  grupo de contestación **4
  contestación directa **5
  parqueo **6
  dnd **7
  rediscado **8
```

Diagnóstico de conectividad de CUE

Aparece la ventana Diagnóstico CUE cuando se selecciona **Solución de problemas** > **CUE Diagnóstico** > **Diagnóstico de conectividad de CUE**.

Antes de ejecutar el diagnóstico CUE:

- Asegúrese que Telnet esté activada en el UC500. Al suar CCA, Telnet siempre está activada.
- Un firewall que se esté ejecutando en su PC puede potencialmente bloquear la conexión entre el módulo CUE en el UC 500 y Configuration Assistant. es posible que necesite desactivar temporalmente el firewall o configurarlo para que permita el acceso al módulo CUE mientras realiza el diagnóstico de CUE.

La ventana Diagnóstico de conectividad de CUE entrega herramientas para el diagnóstico y solución de problemas relacionados con el módulo CUE en el UC500. El sistema de correo de voz de Cisco Unity Express (CUE) y las aplicaciones del UC500, como TimecardView, residen en el módulo CUE del UC500.

En esta ventana, se puede:

- Verifique la conectividad entre la PC que ejecuta CCA y el módulo CUE y visualice la salida de los comandos de modo de ejecuciñon de CUE en una ventana de la consola.

- Ejecute una o más de las siguientes Tareas de recuperación para poner al módulo en un estado conocido para resolver los problemas de CUE (por ejemplo, reinicio continuo o fallos en la actualización de software):
  - Recarga de CUE
  - Cambie a modo de carga de reinicio
  - Arranque de CUE desde la imagen en la memoria flash del UC500
- Gnere un registro de CUE para buscar los problemas de bajo nivel en el módulo CUE

Para saber más acerca de las opciones de diagnóstico de CUE, consulte estas secciones:

- **Verificación de estado, página 635**
- **Generación de registros, página 635**
- **Realización de Tareas de recuperación, página 636**

Verificación de estado

Cuando se hace clic en **Verificar estado**, CCA intenta abrir una conexión Telnet hacia el módulo de CUE para verificar la salud general del módulo. Dependiendo del estado del módulo de CUE, se muestra una salida diferente:

- Si CUE se está inicianco cuando se hace clic en el botón, la salida de progreso del inicio se muestra en la consola.
- Si CUE está activado y en modo de ejecución, se emite el comando **mostrar soporte técnico** y se muestra la salida en la consola.
- Si CUE está en modo de carga de inicio, se emite el comando **mostrar config** y la salida, la que incluye los parámetros de configuración se muestra en la consola.
- Si no puede establecerse la sesión de CUE, se muestra el mensaje de error adecuado en la consola.

Generación de registros

El botón **Generar registros** sólo se activa si CUE está activo y en modo config o de ejecución.

Cuando se hace clic en **Generar registros**, CCA reúne la información de depuración del módulo de CUE y crea un archivo .zip que contiene todos los archivos de registros generados. Estos registros se recopilan:

- install.log
- syslog.log
- atrace_save.log
- debug_server.log
- sshd.log
- postgres.log
- klog.log
- messages.log
- shutdown_installer.log

Se le solicita especificar un directorio de registro por defecto para el archivo .zip.

Realización de Tareas de recuperación

Seleccione una tarea de recuperación y haga clic en **Aceptar**.

PRECAUCIÓN Sólo debería realizar Tareas de recuperación en el módulo de CUE si se lo indica Soporte de Cisco para abordar un problema específico.

La recarga de CUE puede tomar de 10 a 15 minutos.

Al realizar Tareas de recuperación de CUE, el correo de voz, la Contestadora automática y aplicaciones de telefonía, como WebEx PhoneConnect y TimeCardView de Cisco no están disponibles.

Tarea de recuperación	Descripción
Recarga de CUE	La interfaz de CUE se restablece y se muestra el progreso a medida que CUE se está iniciando en la consola.

Tarea de recuperación	Descripción
Ponga CUE en Bootloader	Esta opción intenta poner a CUE en modo de carga de inicio. ESto es útil para poner a CUE en un estado conocido para que se pueda examinar la configuración de inicio y, luego, intentar iniciar CUE desde la imagen en la memoria flash de CUE.
Arranque de CUE desde la imagen en la memoria flash	Esta opción sólo está disponible si CUE está en modo de carga de inicio. La imagen de la memoria flash de CUE se usa para iniciarlo, y el progreso se muestra en la consola.

Diagnóstico de seguridad

Configuration Assistant de Cisco entrega estas herramientas de diagnóstico de seguridad:

- **Registro de depuración de Firewall/NAT**
- **Registro de depuración de VPN**

Registro de depuración de Firewall/NAT

Aparece la ventana Registro de depuración de de Firewall/NAT cuando se selecciona **Solución de problemas** > **Diagnóstico de seguridad** > **Registro de depuración de Firewall/NAT**.

Visión general

La función Registro de depuración de Firewall/NAT permite capturar la información de depuración de IOS de Cisco mientras se soluciona un problema o escenario para la plataforma UC 500 y para los routers seguros de la serie SR500. También puede utilizar esta herramienta para obtener los datos de estado y configuración del firewall y de NAT (Traducción de direcciones de red). La información se recopila en archivos de registro de texto y se guarda en un archivo .ZIP.

La facilidad de depuración de IOS de Cisco y los comandos mostrar se utilizan para reunir la información. Se puede especificar uno o más de estos tipos de datos de depuración relacionados con seguridad para recopilarlos:

- NAT
- Firewall
- Filtro de URL

PRECAUCIÓN La activación de la recopilación de información de depuración de seguridad es intensiva en cuanto a recursos y puede degradar el rendimiento en forma importante. Sólo active la depuración de seguridad por periodos breves y evite los periodos de alta utilización, si es posible.

Por este motivo, toda la depuración de seguridad se desactiva cuando se cierra la ventana Registro de depuración de Firewall/NAT o se cierra Configuration Assistant. Si Configuration Assistant se cierra en forma inesperada, estará desactivada toda la depuración la próxima vez que se inicie Configuration Assistant.

Procedimientos

Para generar un registro sólo de la salida del comando **mostrar**:

PASO 1 En la ventana Registro de depuración de Firewall/NAT, haga clic en **Explorar** y seleccione un directorio de archivos de registro.

PASO 2 Haga clic en **Generar registro de solución de problemas**.

No es necesario seleccionar ninguna opción de depuración de Firewall/NAT ni activar la depuración.

Se crea un archivo de registro de texto en el directorio especificado; no se crea un archivo .ZIP. Este registro incluye la salida de los comandos mostrar relacionados con Firewall/NAT. Una barra de progreso aparece mientras se genera el registro.

PASO 3 Haga clic en **Aceptar** para cerrar la ventana cuando termine de generar el registro.

Para activar la depuración y recopilar los datos de resultado de comandos mostrar y depuración de seguridad:.

PASO 1 En la ventana Registro de depuración de Firewall/NAT, haga clic en **Explorar** y seleccione un directorio de archivos de registro.

PASO 2 Seleccione el tipo se datos de depuración de seguridad para recopilarlos.

PASO 3 Haga clic en **Aplicar depuración** para comenzar a general la inforación de la depuración.

PASO 4 Reproduzca el problema en su red.

PASO 5 Haga clic en **Generar registro de solución de problemas**.

Se crea un archivo .ZIP en el directorio de archivos de registro especificado. Este registro incluye el resultado de los comandos mostrar relacionados con Firewall/NAT y todos los datos de depuración de seguridad. Una barra de progreso aparece mientras se genera el registro.

PASO 6 Haga clic en **Aceptar** para cerrar la ventana cuando termine de generar el registro.

PASO 7 Desactive (desmarque) la depuración de Firewall/NAT y haga clic en **Aceptar** para cerrar la ventana.

Toda la depuración de Firewall/NAT se desactiva automáticamente cuando se cierra la ventana.

Registro de depuración de VPN

Aparece la ventana Registro de depuración de VPN cuando se selecciona **Solución de problemas** > **Diagnóstico de seguridad** > **Registro de depuración de VPN**.

Visión general

La función Registro de depuración de VPN permite capturar la información de depuración de IOS de Csico mientras se soluciona un problema de VPN para la plataforma UC 500 y para los routers seguros de la serie SR500. También se puede utilizar esta herramienta para recopilar la configuración de VPN y datos de su estado. La información se recopila en archivos de registro de texto y se guarda en un archivo .ZIP.

La facilidad de depuración de IOS y los comandos mostrar se utilizan para reunir la información. Se puede especificar uno o más de estos tipos de datos de depuración relacionados con VPN para recopilarlos:

- EZVPN

- VPN de sitio a sitio (IPSec)
- VPN sobre SSL (Sin clientes)
- VPN sobre SSL (Túnel total)

  Si se selecciona VPN sobre SSL (Túnel total), seleccione una ACL, luego especifique un nombre de usuario de VPN de Internet. Las ACL indicadas son las que están configuradas en el router.

PRECAUCIÓN La activación de la recopilación de información de depuración de VPN es intensiva en cuanto a recursos y puede degradar el rendimiento en forma importante. Sólo active la depuración de VPN por periodos breves y evite los periodos de alta utilización, si es posible.

Toda la depuración de VPN se desactiva cuando se cierra la ventana Registro de depuración de VPN o se cierra Configuration Assistant. Si Configuration Assistant se cierra en forma inesperada, estará desactivada la depuración de VPN la próxima vez que se inicie Configuration Assistant.

Procedimientos

Para generar un registro sólo de la salida del comando **mostrar**:

PASO 1 En la ventana Registro de depuración de VPN, haga clic en **Explorar** y seleccione un directorio de archivos de registro.

PASO 2 Haga clic en **Generar registro de solución de problemas**. No es necesario seleccionar ninguna opción de depuración de VPN ni activar la depuración.

Se crea un archivo de registro de texto en el directorio especificado; no se crea un archivo .ZIP. Este registro incluye la salida de los comandos mostrar relacionados con Firewall/NAT. Una barra de progreso aparece mientras se genera el registro.

PASO 3 Haga clic en **Aceptar** para cerrar la ventana cuando termine de generar el registro.

Para activar la depuración y recopilar los datos de resultado de comandos mostrar y depuración de VPN:

PASO 1 En la ventana de REgistro de depuración de VPN, haga clic en **Explorar** y seleccione un directorio de archivo de registro. Seleccione el tipo de datos de depuración de VPN para recopilarlos.

- EZVPN
- VPN de sitio a sitio (IPSec)
- VPN sobre SSL (Sin clientes)
- VPN sobre SSL (Túnel total). Seleccione una ACL (lista de acceso) del menú desplegable o especifique un nombre de usuario de VPN de Internet.

PASO 2 Haga clic en **Aplicar depuración** para comenzar a general la inforación de la depuración.

PASO 3 Reproduzca el problema en su red.

PASO 4 Haga clic en **Generar registro de solución de problemas**.

Se crea un archivo .ZIP en el directorio de archivos de registro especificado. Este registro incluye el resultado de los comandos mostrar relacionados con la depuración de VPN y todos los datos de depuración de seguridad. Una barra de progreso aparece mientras se genera el registro.

PASO 5 Haga clic en **Aceptar** para cerrar la ventana cuando termine de generar el registro.

PASO 6 Desactive (desmarque) la depuración de VPN y haga clic en **Aceptar** para cerrar la ventana. Toda la depuración de VPN se desactiva automáticamente cuando se cierra la ventana.

Depuraciones genéricas

Aparece la ventana Depuración genérica cuando se selecciona **Solución de problemas** > **Depuración genéricas** en la barra de funciones.

Para obtener información acerca de cómo ver información adicional de diagnóstico basado en comandos, consulte **Comandos ejecutables de IOS, página 643** y **Comandos ejecutables de CUE, página 643**.

Visión general

En la ventana Depuración genérica, usted puede: especificar uno o más comandos de depuración de IOS de Cisco, uno por línea, para que se ejecute en el dispositivo. Una vez que se recopilen los datos, se puede ver la salida de depuración en el editor de texto por defecto y guardarla en un archivo o buscar información específica en la salida.

Se excluyen ciertos comandos de depuración intensiva en cuanto a recursos de esta ventana. Configuration Assistant muestra un mensaje si se especifica cualquiera de estos comandos o si el comando especificado es inválido.

La salida se almacena en un búfer de anillo de 5 MB. Cuando la cantidad de datos superior a 5 MB, los datos más antiguos se sobrescriben con los datos más recientes.

Para compilar información de depuración genérica:

PASO 1 Especifique los comandos de depuración de IOS que se ejecutarán en el dispositivo, uno por línea.

PASO 2 Haga clic en **Comenzar** para iniciar la recopilación de información.

PASO 3 Reproduzca el escenario o problema en la red.

PASO 4 Haga clic en **Finalizar** para detener la recopilación de los datos de depuración.

PASO 5 Una vez que se han recopilado los datos, se puede:

- Hacer clic en **Buscar** para buscar el resultado de depuración de búsqueda en el área de resultado de la ventana. La ventana de comandos muestra sólo el resultado de cada comando, y no repite los comandos a medida que éstos se ejecutan.
- Haga clic en **Guardar y mostrar resultado de depuración** para ver el resultado de la depuración en el editor de texto por defecto y guardarlo en un archivo.
- Hga clic en **Borrar listaList** para restablecer la lista de comandos de depuración y especificar diferentes comandos o en un orden diferente.

PASO 6 Haga clic en **Aceptar** para cerrar la ventana. Toda la depuración se desactiva cuando se cierra la ventana. Si Configuration Assistant se cierra en forma inesperada, estará desactivada toda la depuración la próxima vez que se inicie Configuration Assistant.

Comandos ejecutables de IOS

Para ver el resultado de los comandos de modo ejecutable de IOS, seleccione **Solución de problemas**> **Comandos Ejecutables de IOS**.

En la ventana Comandos ejecutables de IOS de Cisco, se puede mostrar simultáneamente el resultado de hasta cuatro comandos de modo ejecutable de IOS. Los comandos pueden seleccionarse de una lista o especificarse manualmente.

- Para mostrar el resultado de un solo comando, seleccione un comando ejecutaable de IOS de Cisco de la lista o especifíquelo manualmente y haga clic en **Ejecutar**.
- Para mostrar el resultado para múltiples comandos, seleccione el número de paneles que se mostrarán (1, 2 ó 4). Especifique o seleccione cada comando y haga clic en **Ejecutar** para mostrar el resultado en un nuevo panel. Si todos los paneles están en uso, el resultao del próximo comando que se ejecute sobreescribirá el resultado del comando más antiguo.
- Haga clic en **Borrar paneles** para borrar todos los paneles abiertos.
- Haga clic en **Actualizar** para actualizar la información indicada en cada panel.

Comandos ejecutables de CUE

Para ver el resultado de los comandos de modo ejecutable de CUE, seleccione **Solución de problemas**> **Comandos Ejecutables de CUE**.

En la ventana Comandos ejecutables de CUE, se puede mostrar simultáneamente el resultado de hasta cuatro comandos de modo ejecutable de CUE. Los comandos pueden seleccionarse de una lista o especificarse manualmente.

- Para mostrar el resultado de un solo comando, especifíquelo manualmente y haga clic en **Ejecutar**.
- Para mostrar el resultado para múltiples comandos de modo ejecutable de CUE, seleccione el número de paneles que se mostrarán (1, 2 ó 4). Especifique cada comando y haga clic en **Ejecutar** para mostrar el resultado en un nuevo panel. Si todos los paneles están en uso, el resultao del próximo comando que se ejecute sobreescribirá el resultado del comando más antiguo.

- Haga clic en **Borrar paneles** para borrar todos los paneles abiertos.
- Haga clic en **Actualizar** para actualizar la información indicada en cada panel.

Generación de un registro de soluciones de problemas del sistema

Realice estos pasos para recopilar la información de solución de problemas desde dentro de Configuration Assistant para ayudar al TAC a resolver estos problemas.

Puede seleccionar un UC500 o un SR500 como el dispositivo, si se configura un sitio de clientes.

PASO 1 Desde dentro de CCA, seleccione **Ayuda** > **Información de soporte** del menú de la parte superior de la ventana principal.

PASO 2 En la ventana Información de soporte, haga clic en **Registro de soluciones de problemas**.

PASO 3 Haga clic en **Explorar** y seleccione cualquier carpeta de su PC para el directorio de archivos de registro.

PASO 4 En el campo Nombre de host, seleccione el dispositivo UC500 ó SR500 de la comunidad.

PASO 5 Haga clic en **Generar registro**.

Configuration Assistant recopila los archivos de registro y de configuración requeridos para la solución de problemas.

Este proceso puede tardar hasta 5 minutos. El archivo de registro se crea en la carpeta especificada en el paso 3.

PASO 6 Adjunte este archivo de registro a su caso de TAC (Centro de asistencia técnica de Cisco) para el soporte técnico.

El nombre del archivo de registro y su formato es UC5*x*0_*Dirección MAC*_*Fecha*_*Hora*_tac_logs.zip.

Enlaces y Conectividad (switches CE520)

Para probar los enlaces y detectar problemas de conectividad en un sistema con una switch CE520, seleccione Enlaces y conectividad en la barra de funciones.

Visión general

En la ventana Enlaces y Conectividad, se puede descubrir estos tipos de problemas en su red:

- No existe conectividad entre un dispositivo de origen y un dispositivo de destino.
- No hay cable o hay un cable con fallas conectado al puerto.
- No hay coincidencia en la configuración de velocidad del puerto en un enlace.
- Problemas de conectividad entre dos dispositivos de la red, por ejemplo, un host y un servidor.

NOTA La prueba de conectividad sólo es admitida en los puertos Ethernet 10/100/1000 de cobre.

Procedimientos

Para agregar un enlace, siga estos pasos:

PASO 1 Seleccione **Enlace (Servicio perjudicial)** de la lista **Tipo de prueba**.

PASO 2 Seleccione un nombre del host de la lista Nombre del host.

PASO 3 Seleccione una interfaz de la lista Interfaz o haga clic en el icono junto al campo Interfaz y seleccione una interfaz en el dispositivo desplegado.

PASO 4 Haga clic en **Iniciar** para comenzar la prueba.

En caso de que exista algún error en el enlace, la descripción del mensaje de error y la recomendación aparecen en el área Resultados. Si no hay errores, aparece un mensaje que indica que no hay errores.

Para resolver un problema en el enlace, haga clic en el botón **Repararlo**. Sólo es posible reparar un problema de diferencia en la velocidad usando Configuration Assistant.

Para probar la conectividad de la red entre dos dispositivos, es necesario que proporcione la dirección IP de origen de un dispositivo y la dirección IP de destino del otro dispositivo. Los resultados de la prueba muestran si existe conectividad entre los dispositivos.

Para probar la conectividad de la red entre dos dispositivos:

PASO 1 Seleccione **Conectividad** de la lista Tipo de prueba.

PASO 2 En el campo Dirección **IP de origen**, especifique la dirección IP de origen de uno de los dispositivos.

PASO 3 En el campo Dirección **IP de destino**, especifique la dirección IP de destino del otro dispositivo.

Haga clic en **Iniciar** para comenzar la prueba. La descripción del mensaje y la recomendación aparecen en el área Resultados.

A

Dónde ir desde aquí

Cisco entrega una amplia gama de recursos para ayudarle a usted y a sus clientes a obtener todos los beneficios de Cisco Configuration Assistant y el Sistema Cisco Smart Business Communications System (SBCS).

Cisco Configuration Assistant	
Cisco Configuration Assistant Página del producto	www.cisco.com/go/configassist
Documentación técnica de Configuration Assistant de Cisco	www.cisco.com/en/US/products/ps7287/tsd_products_support_series_home.html
Pautas de configuración fuera de banda para Cisco Configuration Assistant	http://www.cisco.com/en/US/partner/products/ps7287/prod_installation_guides_list.html
Cisco Small Business	
Central de socios para pequeñas empresas de Cisco (Debe iniciar sesión como socio)	www.cisco.com/web/partners/sell/smb
Inicio de Cisco Small Business	www.cisco.com/smb
Cisco Small Business Support	
Comunidad de soporte para pequeñas empresas de Cisco	www.cisco.com/go/smallbizsupport
Soporte y recursos para pequeñas empresas de Cisco	www.cisco.com/go/smallbizhelp
Contactos para soporte por teléfono	www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html
Descargas de firmware para pequeñas empresas de Cisco	www.cisco.com/go/smallbizfirmware Seleccione un enlace para descargar firmware para los productos para pequeñas empresas de Cisco. No se necesita iniciar sesión. Las descargas para todos los productos para pequeñas empresas de Cisco, incluyendo los Sistemas de almacenamiento en red, están disponibles en el área de Descargas de Cisco.com en www.cisco.com/go/software (se necesita registro/inicio de sesión).

Sistema y componentes de comunicaciones Smart Business de Cisco	
Archivos de localización y paquetes de software del UC500 de Cisco (Inicio de sesión en Cisco.com necesario)	www.cisco.com/go/uc500swpk
Sistema de comunicaciones de Smart Business de Cisco	www.cisco.com/go/sbcsresources
Serie Unified Communications 500 de Cisco	www.cisco.com/go/uc500resources
Teléfono IP de Cisco serie SPA500	www.cisco.com/go/spa500phones
Teléfonos IP de Cisco serie SPA300	www.cisco.com/go/300phones
Teléfonos IP unificado de Cisco serie 7900	www.cisco.com/en/US/products/hw/phones/ps379/
Punto de acceso AP541N de Cisco	www.cisco.com/go/ap500resources
Dispositivo de seguridad SA500 de Cisco	www.cisco.com/go/sa500resources
Switches de la serie ESW500 de Cisco	www.cisco.com/go/esw500resources
Cámaras de vídeo para empresas PVC2300 (Audio/PoE) y WVC2300 (Audio/Wireless-G) de Cisco	www.cisco.com/go/smallbizcameras
Router seguro serie SR500 de Cisco	www.cisco.com/go/sr500
Guía de referencia de funciones del Sistema Smart Business Communications System	www.cisco.com/en/US/partner/prod/collateral/voicesw/ps6882/ps10585/partner_reference_c07-557625-00.html
Avisos de licencia	
Abrir avisos de fuente abierta	www.cisco.com/go/osln El Aviso de licencia de fuente abierta para CCA 3.0 se ubica en una página de descarga de software para CCA en Cisco.com.

Glosario

A

AAA	Autenticación, autorización y cuentas. Pronounced “triple-A.”
ABR	Router del borde del área. Un router que se localiza en el borde de una o más áreas OSPF y que conecta las áreas a la red troncal. Los ABRs se consideran miembros tanto de áreas adjuntas como de troncales OSPF. Por lo tanto, ellos mantienen tablas de enrutamiento que describen la topología troncal y la topología de las áreas.
punto de acceso	Un dispositivo que sirve como un punto central en una red inalámbrica o como un punto de conexión entre dispositivos inalámbricos y una red cableada. Consulte también el punto de acceso autónomo y el LAP (punto de acceso liviano)
puerto de acceso	Un puerto que lleva el tráfico de una LAN virtual (VLAN). Contraste con el puerto troncal.
VLAN de acceso	Una VLAN que es usada por un switch para tráfico de datos. Consulte también VLAN nativa y VLAN de voz.
Agrupación de direcciones	Una función de protocolo de enrutamiento que interrumpe las principales direcciones de red para agregar grupos contiguos de representación numérica de direcciones conocidos como superredes. Esta función suprime automáticamente los anuncios de redes más específicas en una interfaz elegida.
anuncio	El proceso del router de enviar actualizaciones de servicio y enrutamiento a intervalos de modo que otros routers puedan mantener una tabla de rutas de uso.
máscara de dirección	Una combinación bit usada para describir qué parte de una dirección se refiere a la red o la subred y qué parte se refiere al host. Consulte también dirección IP y máscara de subred.

velocidad administrativa	La velocidad de un enlace como especifica el administrador. Si el administrador especifica la velocidad como automática, la velocidad real se determina a través de negotiación automática.
AES	Estándar de cifrado avanzado. Un cifrador de bloques que puede cifrar y descifrar los datos utilizando claves de 128.192, 192 ó 256 bits.
AES CCMP	Modo de Contador estándar de cifrado avanzado con Protocolo de código de autenticación de mensajes en cadena de bloque de cifrador. Un protocolo que utiliza AES. El algoritmo CCMP genera un código de integridad de mensajes que entrega autenticación de origen de datos e integridad de datos para el paquete inalámbrico.
Interfaz de administrador AP	Una interfaz que se utiliza para todas las comunicaciones de capa 3 entre un controlador de WAN y puntos de acceso livianos (LAP) después que éstos se han unido al controlador de WAN.
ARP	Protocolo de resolución de direcciones. Un protocolo de Internet que se usa para trazar un mapa de una dirección IP a una dirección MAC.
Área	Un grupo de routers adyacentes que comparten actualizaciones del estado del enlace OSPF. Es identificado por un número conocido como un ID de área.
ATM	Modo de transferencia autónoma. El estándar internacional para el relé de celda en el cual tipos de servicio múltiples (tales como voz, vídeo, o datos) se transportan en celdas de longitud fija (53 bits). Las celdas de longitud fija permiten que el procesamiento de celda ocurra en el hardware, así se reducen los retrasos del tránsito. ATM está diseñado para obtener ventaja de los medios de transmisión de alta velocidad, tales como E3, SONET y T3.
Negociación automática	La capacidad de los puertos enlazados de determinar las características de cada uno y de elegir el mejor método de comunicación.
Punto de acceso autónomo	Un punto de acceso independiente con todas las funciones que no necesita un controlador de WAN para funcionar. Comparar con LAP (punto de acceso liviano.
AWP	Puertos cableados de modo alternativo. Dos puertos físicos que operan como un puerto lógico único. Usualmente un puerto usa un conector de fibra SFP y el otro puerto usa un conector de cobre RJ45.

B

BOOTP Protocolo Bootstrap. El protocolo usado por un nodo de red para determinar la dirección IP de sus interfaces Ethernet para afectar arranque de la red.

C

CAC Control de Admisión de llamadas (Call Admission Control). Un proceso de regulación de calidad de la voz que limita el número de llamadas que pueden estar activas en un enlace en particular al mismo tiempo. CAC no garantiza un nivel particular de calidad de audio en el enlace, pero no permite regular la cantidad de ancho de banda que consumen las llamadas activas en el enlace.

CAS Señalización asociada a canales. La transmisión de información de señalización dentro del canal de voz. A la señalización CAS con frecuencia se le hace referencia como señalización de bit robado, ya que el ancho de banda del usuario está siendo robado por la red para otros propósitos.

CCKM Administración centralizada de claves de Cisco. Un protocolo que soporte apalicaciones sensibles a la hora como un voz sobre IP (VoIP) inalámbrico. CCKM utiliza una técnica de repetiticón de claves que permite que los clientes se desplacen desde un punto de acceso a otro sin pasar por el controlador.

CDP Protocolo de descubrimiento de Cisco. Un protocolo que un dispositivo usa para anunciar su existencia a otros dispositivos y recibir informaciÃ³n sobre otros dispositivos en la misma LAN o en el lado remoto de una WAN.

CEF Cisco Express Forwarding. Una avanzada tecnología de conmutación de Capa 3 para IP. CEF optimiza el desempeño de la red y la escalabilidad para redes con patrones de tráfico dinámicos y grandes, como los asociados con Internet, aplicaciones basadas en Internet y sesiones interactivas.

CGMP	Protocolo de gestión de grupo de Cisco. Un protocolo que reduce el flooding de paquetes de multidifusión IP al limitar la transmisión de estos paquetes a clientes que los solicitan. Las estaciones finales se transforman en clientes al enviar mensajes adjuntos para unirse a un grupo CGMP; ellas envían mensajes de abandono para dejar el grupo.
modo sin clientes	Entrega un acceso seguro a los recursos privados de la web y acceso al contenido de ella.
sitio de cliente	Un grupo de dispositivos que se administra por medio de las direcciones IP de sus miembros. Switches, routers, controladores de acceso inalámbrico y puntos de acceso autónomos pueden ser miembros.

D

gateway por defecto	Un nodo de una red que sirve tanto como un punto de salida hacia otra red como punto de entrada desde otra.
discado con retraso	El extremo de origen toma la línea y espera 200 ms para ver si el otro extremo está descolgado o no. Si no es así, el extremo de origen pulsa dígitos. Si el otro extremo está descolgado, el extremo de origen espera hasta que el otro extremo esté colgado antes de pulsar los dígitos.
envío basado en el destino	El envío de un paquete por un grupo de puertos basado en la dirección de destino del paquete. Contraste con el envío basado en el origen.
DHCP	Protoclo de configuración dinámica del host. Un mecanismo para asigar dinámicamente direcciones IP de modo que las direcciones se pueden volver a utilizar cuando los hosts no las necesitan más.
DID	Discado interno directo. Un servicio ofrecido por las empresas telefónicas que permite a quien llama discar directamente un anexo en un PBX o sistema de voz sin la asistencia de una operadora ni de un asistente de llamadas automático. Este servicio utiliza los enlaces DID, que envían sólo los últimos tres a cinco dígitos de un número telefónico a la PBX o al router/ gateway.
autenticación digest	Un proceso para enlaces y teléfonos SIP que permite desafiar la identidad de un agente usuario (UA) SIP cuando éste envía una solicitud. (Un agente usuario representa un dispositivo o aplicación que origina un mensaje SIP).

DMZ Zona desmilitarizada. Una zona de búfer entre Internet y sus redes privadas. Puede ser una red pública utilizada generalmente para servidores de Internet, FTP y correo electrónico a los cuales se accede mediante clientes externos en Internet. Ubicar estos servidores de acceso público en redes aisladas separadas proporciona una medida de seguridad adicional para una red interna.

DNS Servicio de nombre de dominio. Un servicio de Internet que traduce los nombres de dominio, que están compuestos por letras, en direcciones IP, que están compuestas por números.

nombre de dominio El nombre familiar y fácil de recordar de un host en Internet que corresponde a su dirección IP.

dirección dinámica Una dirección MAC que se reconoce en un puerto. Se almacena en la tabla de direcciones y se pierde cuando el switch se recarga. La primera dirección MAC que se reconoce cuando la seguridad del puerto se activa se transforma en una dirección dinámica segura. Vea también dirección estática.

enrutamiento dinámico Enrutamiento que se ajusta automáticamente a la topología de la red o cambios de tráfico. También se denomina enrutamiento adaptable.

E

EANA Acceso igualitario norteamericano. Una de cuatro formas comunes de señalización CAS; las otras son inicio de tierra, inicio en bucle y E&M.

EAP Protocolo de autenticación extensible. Un método de autenticación en el que un punto de acceso asiste a un dispositivo cliente inalámbrico y a un servidor RADIUS para que realice la autenticación y derive una clave dinámica WEP.

EIGRP Protocolo de enrutamiento interior mejorado para gateway. Una versión de Cisco de IGRP que entrega propiedades de convergencia superiores y eficiencia de operación y combina las ventajas de protocolos del estado del enlace con aquellas de protocolos de vector de distancia.

E&M Una de cuatro formas comunes de señalización CAS; las otras son inicio desde cero, inicio en bucle y EANA.

punto final Un terminal o gateway SIP. Un punto final puede llamar u recibir llamadas. Genera y/o interrumpe el flujo de información.

EtherChannel	Un grupo de puertos Fast Ethernet o Gigabit Ethernet que actúa como un puerto lógico único para conexiones de ancho de banda mayor entre switches o entre switches y servidores. Si un puerto dentro de un EtherChannel falla, el tráfico previamente llevado en los puertos defectuosos se transfiere a los puertos restantes dentro del EtherChannel.
Puerto de administración de Ethernet	El puerto de administración de Ethernet es un puerto de host de 3 capas que se puede conectar a una PC. Es posible utilizar el puerto de administración de Ethernet en vez del puerto de la consola del switch para la administración de la red. Este puerto se debe utilizar sólo para administrar el switch. El puerto de administración de Ethernet admite la configuración de puerto y las funciones de dirección IP en Configuration Assistant de Cisco.
EZVPN	Easy VPN Solución de administración VPN centralizada que se basa en Unified Client Framework de Cisco. Easy VPN de Cisco está compuesta por dos componentes: un cliente remoto Easy VPN de Cisco y un servidor Easy VPN de Cisco.

F

recuperación tras fallo	La transferencia de responsabilidades a un switch standby.
Fast Leave	Una función de enrutamiento de multidifusión que acelera la remoción de un grupo de multidifusión de un router. Cuando un miembro deja un grupo, Fast Leave busca otros miembros del grupo (dispositivos que reciben paquetes de multidifusión IP desde un puerto particular en el switch). Si no existen otros miembros en el puerto, el switch remueve el puerto del grupo. Si no existen otros puertos en el grupo, el switch notifica los routers conectados a la VLAN para eliminar el grupo entero.
firewall	Un router o servidor de acceso o diversos routers o servidores de acceso, diseñaados como búfer entre redes públicas conectadas y una red privada. Un router de firewall utiliza listas de acceso y otros métodos para asegurar la seguridad de la red privada.
FTP	Protocolo de transferencia de archivos. Parte de la pila de protocolos TCP/IP, utilizada para transferir archivos entre hosts.

G

GBIC
Conversor de interfaz Gigabit. Un emisor-receptor que convierte corrientes eléctricas (digitales altas y bajas) en señales ópticas y señales ópticas en corrientes eléctricas digitales. El GBIC se usa típicamente en sistemas de Ethernet y fibra óptica como una interfaz para sistemas de red de alta velocidad. La velocidad de transferencia de datos es de 1 Gigabit por segundo (1 Gbps) o más.

intervalo de encuesta de gráfico
La frecuencia con la que Configuration Assistant consulta a los miembros de una comunidad para obtener datos de utilización por enlace y por dispositivo a través de un grupo de dispositivos. Esta información se usa para actualizar gráficos enlace y de ancho de banda. Consulte también el intervalo de encuesta de estado, intervalo de encuesta de LED e intervalo de encuesta de la red.

GRE
Encapsulamiento de enrutamiento genérico. Un protocolo de arquitectura de túneles que encapsula una variedad de tipos de paquetes de protocolos dentro de túneles IP, creando una conexión virtual de punto a punto hacia dispositivos en puntos remotos sobre una red IP. Con esta tecnología, GRE encapsula el paquete original completo con un encabezado IP estándar y un encabezado GRE antes del proceso IPSec. Luego, IPSec ve al paquete GRE como un paquete IP no notable y realiza los servicios de cifrado y autentificación, según lo dictan los parámetros negociados IKE. Debido a que GRE puede llevar tráfico de disfusión y de multidifusión, es posible configurar un protocolo de enrutamiento para los túneles GRE virtuales. El protocolo de enrutamiento detectga la pérdida de conectividad y vuelve a enrutar los paquetes hacia el túnel GRE de copia de seguridad, entregando con ello una alta resiliencia.

groundstart
Una de cuatro formas comunes de señalización T1 CAS. Es principalmente una señal analógica que puede utilizarse en FXS, FXO o cualquier puerto analógico; los otros son EANA y E&M.

H

intervalo de encuesta de estado
La frecuencia con la que Configuration Assistant consulta a los dispositivos de un sitio de cliente para obtener datos del uso de los recursos y temperaturas de los dispositivos. Consulte también el intervalo de encuesta de gráficos, intervalo de encuesta de LED e intervalo de encuesta de la red.

red inicial La red en el sector del servidor de un túnel VPN. Por ejemplo, un invitado en una noche podría conectar un PC a la red del hotel para descargar un archivo almacenado en un servidor ubicado físicamente en la red corporativa del invitado. La conexión se establece desde la red del hotel a través de Internet a la red corporativa al usar un túnel VPN. En este ejemplo, la red del hotel es la red remota y la red corporativa es la red inicial.

grupo de búsqueda Número de líneas telefónicas que se asocian juntas por parte de la oficina central de la compañía de teléfonos o un sistema PBX. Cuando llega una llamada a un grupo de búsqueda, recorre el grupo de líneas hast que encuentre una desocupada y luego hace sonar ese teléfono (o anexo, si es un sistema PBX).

HSRP Protocolo de enrutamiento Hot Standby. Un protocolo que entrega disponibilidad de red alta y cambios de topología de red transparentes. Crea un grupo de dispositivos con un dispositivo principal que sirve a todos los paquetes enviados a una dirección hot standby. El dispositivo principal es monitoreado por otros en el grupo; si falla, uno de los otros dispositivos hereda la posición principal y la dirección hot standby.

HWIC Tarjeta de interfaz WAN de alta velocidad. Una tarjeta de interfaz de LAN inalámbrica en el form-factor HWIC que entrega funcionalidad de punto de acceso integrado en los dispositivos Cisco con capacidade enrutamiento.

I

ICMP Protocolo de mensajes de control de Internet. Un protocolo de Internet de capa de red que informa errores y entrega otra información relevante al procesamiento de paquetes IP.

IGMP Protocolo de gestión de grupo Cisco. Un protocolo que se usa entre hosts y routers en la LAN para determinar a qué grupos de multidifusuón pertenecen los hosts.

snooping IGMP El examen efectuado por un switch de 2 capas de alguna información de 3 capas en un paquete IGMP enviada desde un host a un router. El switch determina a partir de sus hallazgos si se debe agregar o remover puertos miembro.

IGRP Protocolo de enrutamiento interior para gateway. Un Protocolo interior para gateway que dirige emisiones asociadas con el enrutamiento en grandes redes heterogéneas.

IKE	Intercambio de claves por Internet. Un protocolo estándar de administración de claves usado en conjunto con IPsec y otros estándares. IPsec puede configurarse sin IKE, pero IKE mejora IPsec al proporcionar funciones adicionales, flexibilidad y facilidad de configuración para el estándar IPsec. IKE proporciona autenticación de los pares IPsec, negocia claves IPsec y negocia asociaciones de seguridad IPsec.
Immediate Leave	Una función de enrutamiento de multidifusión que acelera la remoción de un grupo de multidifusión de un router. Cuando un miembro indica que desea dejar el grupo, la Immediate Leave remueve el puerto de miembro del grupo de inmediato.
inicio inmediato	El extremo de origen toma la línea al descolgarla y, sin esperar respuesta, comienza a pulsar dígitos.
interfaz interna	La primera interfaz que conecta el dispositivo a su red interna fiable protegida por un dispositivo de seguridad.
Su dirección IP	Una dirección de 32 bits asignada a hosts que usan TCP/IP. Pertenece a una de cinco clases (A, B, C, D o E) y está escrita en cuatro octetos separados por puntos (formato decimal de puntos). Cada dirección consiste en un número de red, un número de subred opcional y un número de host. Los números de redes y subredes juntos se usan para el enrutamiento, y el número de host se usa para dirigir un host individual dentro de la red o subred. Para extraer información de redes y subredes desde una dirección IP se usa una máscara de subred.
Teléfono IP	Teléfonos con todas las funciones que entrega comunicación de voz en una red IP.
IPsec	Un marco de estándares abiertos que proporciona confidencialidad de datos, integridad de datos y autenticación de datos entre pares participantes. IPsec proporciona estos servicios de seguridad en el nivel IP. IPsec utiliza IKE para administrar la negociaciÃ³n de protocolos y algoritmos basados en políticas locales y para generar las claves de cifrado y autenticación que serán usadas por IPsec. IPsec se puede utilizar para proteger uno o más flujos de datos entre un par de hosts, entre un par de gateway de seguridad o entre una gateway de seguridad y un host.
ISL	Enlace entre switch. Un protocolo de propiedad de Cisco que mantiene la información de VLAN como flujos de tráfico entre switches y routers.

K

sistema de claves	Un sistema telefónico a pequeña escala diseñado para manejar comunicaciones telefónicas en oficinas pequeñas de 1 a 25 usuarios. Los sistemas de claves pueden ser analógicos o digitales. En un sistema de claves, cada teléfono puede responder cualquier llamada PSTN entrante en cualquier línea. Cuando hay múltiples llamadas en el sistema al mismo tiempo, cada llamada es visible y se puede seleccionar directamente al presionar el botón de línea correspondiente en un teléfono IP.

L

LACP	Protocolo de control de agregado de enlace. El protocolo que apoya la especificación IEEE 802.3AD para reunir interfaces físicas para formar una interfaz lógica única.
Intervalo de encuesta de LED	La frecuencia con la cual Configuration Assistant encuesta a los puertos en un sitio y muestra los cambios en los colores de LED de los puertos. Consulte también el intervalo de encuesta de gráficos, intervalo de encuesta de estado e intervalo de encuesta de la red.
punto de acceso liviano	Un punto de acceso que no puede actuan en forma independiente de un controlador de WAN. El controlador de WLAN gestiona las configuraciones AP y el firmware. No es necesario realizar una configuración individual de estos puntos de acceso. Gestionan sólo la funcionalidad MAC en tiempo real y dejan que la funcionalidad MAC que no es en tiempo real sea procesada por el controlador de WLAN. Esta arquitectura se conoce como la arquitectura de *MAC dividida*. Compare con punto de acceso autónomo.
protocolo de estado del enlace	Un tipo de protocolo de enrutamiento que mantiene un mapa de la intrared, permitiéndole ver rutas alternativas o rutas paralelas para equilibrar la carga. OSPF es un ejemplo de este tipo de protocolo. Contraste con protocolo de vector de distancia.
LEAP	Protocolo liviano de autenticación extensible. Un tipo de autenticación 802.1X para LAN inalámbricas que admita una autenticación mutua y fuerte entre el cliente y un servidor RADIUS utilizando una contraseña de inicio de sesión como la clave secreta compartida. Entrega claves de cifrado dinámicas por usuario y por sesión.

protocolo de estado del enlace	Un tipo de protocolo de enrutamiento que mantiene un mapa de la intrared, permitiéndole ver rutas alternativas o rutas paralelas para equilibrar la carga. OSPF es un ejemplo de este tipo de protocolo. Contraste con protocolo de vector de distancia.
SPAN local	Una sesión de SPAN en la cual todos los puertos de destino y origen están en el mismo switch. Contraste con el SPAN remoto.
inicio de bucle	Una de cuatro formas comunes de señalización T1 CAS, pero es principalmente una señal analógica que puede utilizarse en FXS, FXO o cualquier puerto analógico; los otros son inicio de tierra, EANA y E&M.

M

MAC	Control de acceso de medios. La más baja de las dos subcapas de la capa de enlace de datos definida por el IEEE. La subcapa MAC determina el acceso a medios compartidos, tales como el uso de un paso token o contención.
Su dirección MAC	La dirección de la capa de enlace de datos estandarizada que se requiere para cada puerto o dispositivo que se conecta a una LAN. Otros dispositivos en la red usan estas direcciones para localizar puertos específicos en la red y crear y actualizar tablas de enrutamiento y estructuras de datos. Las direcciones MAC tienen 6 bits de longitud y son controladas por el IEEE.
Interfaz de gestión	La interfaz por defecto para administrar un dispositivo Control de acceso de medios. La más baja de las dos subcapas de la capa de enlace de datos definida por el IEEE. La subcapa MAC determina el acceso a medios compartidos, tales como el uso de un paso token o contención.
enrutamiento de multidifusión	Una técnica de enrutamiento que permite pasar copias de un paquete único a un subconjunto seleccionado de todos los posibles destinos. Contraste con enrutamiento de unidifusión.
Servidor MWI	El servidor MWI de SIP (indicador de mensaje en espera) es un servidor proxy que retarda los mensajes MWI de SIP.

N

NAT	Traducción de direcciones de la red Mecanismo para reducir la necesidad de direcciones IP únicas en todo el mundo. NAT permite una organización con direcciones IP que no sean únicas en todo el mundo para conectar a Internet al traducir estas direcciones en direcciones IP enrutables en todo el mundo.
VLAN nativa	La VLAN que lleva paquetes sin etiqueta desde un puerto troncal IEEE 802.1Q. Consulte también VLAN de acceso y VLAN de voz.
EAP de red	Un método de autenticación en el que el punto de acceso asiste a un dispositivo cliente inalámbrico y al servidor RADIUS para que realicen la autenticación y deriven una clave dinámica WEP.
intervalo de encuesta de red	La frecuencia con que Configuration Assistant encuesta a los miembros de un sitio de cliente para determinar el estado de un grupo de dispositivos y la existencia de nuevos miembros. Consulte también el intervalo de encuesta de gráficos, intervalo de encuesta de estado e intervalo de encuesta deLED.
puerto de red	Un puerto al cual el switch envíaa todo el tráfico de VLAN con direcciones de destino desconocidas; este proceso ayuda a evitar la inundación de todos los puertos en una VLAN.
nombre de notificación	El nombre de una recolección de información que especifica tipos de eventos de sistema y dirección de e-mail a la cual se envía la notificación de estos eventos.
NTP	Protocolo de hora de la red. Un protocolo que asegura la mantención del tiempo local exacto con referencia a la radio y relojes atómicos localizados en la Internet.

O

autenticación abierta	Un método de autenticación que permite que cualquier dispositivo se autentique, y que luego, intente comunicarse con el punto de acceso.
autenticación abierta con EAP	Un método de autenticación en el que el punto de acceso obliga a todos los dispositivos clientes a realizar una autenticación EAP antes que puedan unirse a la red.

OSPF	Abrir ruta más corta primero. Un protocolo del estado del enlace que no impone límites en el conteo de saltos, propaga los cambios de enrutamiento instantáneamente, admite las máscaras de subredes de longitud variable, y permite el equilibrio de la carga basado en el costo real del enlace. Éste también divide las redes en regiones menores llamadas áreas, que limitan el tráfico provocado por las actualizaciones del estado del enlace.
interfaz externa	La primera interfaz, generalmente el puerto 0, que se conecta a otras redes no fiables fuera del dispositivo de seguridad; WAN o Internet.

P

PAT	Traducción de direcciones de puerto. Conserva direcciones en el conjunto global de direcciones al permitir que se traduzcan los puertos de origen en conexiones TCP o conversaciones UDP. Direcciones locales diferentes luego asigna a la misma dirección global con traducción de puerto que proporciona la exclusividad necesaria. Las direcciones del conjunto global se utilizan siempre antes que se utilice una dirección PAT.
grupo de contestación	Esta función permite que los administradores asocien grupos de selección a teléfonos IP individuales, facilitando que los usuarios respondan, o tomen, una llamada que está sonando en una extensión o número de teléfono diferente.
PBX	Intercambio de sucursales privadas. Tablero telefónico digital o analógico ubicado en las instalaciones del suscriptor y usado para conectar redes telefónicas públicas y privadas.
PKI	infraestructura de clave pública. Sistema de autoridades de certificación (CA) y autoridades de registro (RA) que proporciona ayuda para el uso de criptografía de claves asimétricas en comunicación de datos mediante estas funciones como administración de certificados, administración para archivar, administración de claves y administración de token. En forma alternativa, cualquier estándar para el intercambio de claves asimétricas. Este tipo de intercambio permite al destinatario de un mensaje confiar en la firma de ese mensaje y permite al remitente de un mensaje encriptarlo en forma adecuada para el destinatario deseado. Consulte administración de claves.
PPPoE	Protocolo punto a punto en Ethernet. PPP encapsulado en tramas de Ethernet. PPPoE permite a los hosts en una red Ethernet conectarse a hosts remotos a través de un módem de banda ancha.
PoE	Power over Ethernet. Una tecnología que entrega energía a dispositivos conectados a través de cables de datos en vez de cordones de energía.

Intervalo de encuesta Consulte el intervalo de encuesta de gráficos, intervalo de encuesta de LED e intervalo de encuesta de la red.

clave previamente compartida Un método de autenticación ofrecido en IPsec. Claves previamente compartidas permiten a uno o más clientes utilizar secretos individuales compartidos para autenticar túneles encriptados a una gateway usando IKE (Intercambio de claves por Internet). Las claves previamente compartidas se utilizan por lo general en redes pequeñas de hasta 10 clientes. Con las claves previamente compartidas, no hay necesidad de incluir una autoridad de certificación por razones de seguridad.

nivel de privilegio Un número que determina el nivel de acceso de Configuration Assistant que se entrega a un usuario. El nivel 15 le otorga acceso de lectura y escritura; los niveles desde el 1 al 14 otorgan acceso de sólo lectura.

PSTN Red telefónica conmutada pública. Término general referido a la variedad de redes telefónicas y servicios establecidos mundialmente.

Q

QoS Calidad de servicio. Se refiere a la capacidad de una red de entregar un mejor servicio al tráfico de la red seleccionada. La meta principal de QoS es dar prioridad, incluyendo ancho de banda dedicado, control de oscilaciones y latencia (exigido por algún tráfico interactivo y de tiempo real) y mejorar las características de pérdidas.

R

RADIUS Servicio de usuario de acceso telefónico de Autentificación Remota (Remote Authentication Dial-In User Service). Una base de datos para la autentificación del módem y conexiones ISDN y para hacer seguimiento del tiempo de conexión.

red remota La red en el sector del servidor de un túnel VPN. Por ejemplo, un invitado en una noche podría conectar un PC a la red del hotel para descargar un archivo almacenado en un servidor ubicado físicamente en la red corporativa del invitado. La conexión se establece desde la red del hotel a través de Internet a la red corporativa al usar un túnel VPN. En este ejemplo, la red del hotel es la red remota y la red corporativa es la red inicial.

SPAN remoto	Una sesión SPAN en la cual los puertos de origen se localizan remotamente del switch que contiene el puerto de destino. Contraste con el SPAN local.
RIP	Protocolo de información de enrutamiento. El protocolo interior para gateway más común en Internet. Utiliza un conteo de saltos como una métrica de enrutamiento.
Puerto de raíz	El puerto de switch con la mejor ruta al switch de raíz.
switch de raíz	El switch seleccionado para ser el centro de una topologÃa de spanning-tree. El flujo de todos los datos a través de la red se realiza desde la perspectiva de este switch..
interfaz enrutable	Un puerto enrutado o una SVI.
protocolo de enrutamiento	Un conjunto de reglas y convenciones para reunir información sobre redes disponibles, tales como la distancia o costo para alcanzarlas, y determinar la ruta de enrutamiento para un paquete.

S

dirección segura	Una dirección MAC que se envía a sólo un puerto por VLAN. Las direcciones seguras se conservan incluso cuando el switch se recarga. Consulte también dirección dinámica y dirección estática.
puerto seguro	Un puerto para el cual una acción especificada por el usuario ocurre cada vez que se viola la seguridad de la dirección.
SDP	1. Protocolo de descripción de sesión. Un protocolo para definir información necesaria para establecer un transporte multimedia por IP. SDP transmite información, como anuncio de sesiones, invitación de sesiones, direcciones de transporte y tipos de medios. Por ejemplo, en una llamada SIP, los mensajes SDP indican si se utiliza NTE, cuáles eventos enviar utilizando NTE y el valor del tipo de carga útil de NTE. 2. Provisionamiento seguro de dispositivos. Implementa PKI (infraestructura de clave pública) entre dos dispositivos finales, como un cliente IOS de Cisco y un servidor de certificado IOS de Cisco.
SFP	Small form-factor pluggable. Un módulo emisor-receptor óptico láser de campo reemplazable. Los módulos SFP entregan conexiones de enlace de Gigabit a otros switches.

SFTP	Protocolo de transferencia de archivos SSH. SFTP es parte de SSH y siempre está activado en el router. Un usuario con el nivel adecuado puede copiar archivos desde y hacia el router al utilizar SFTP.
Autentificación compartida	Un método de autentificación en le que el punto de acceso envía una cadena de texto de desafío no cifradas a cualquier dispositivo que intente comunicarse con él. Si el texto de desafío está cifrado correctamtente, el punto de acceso permite que el dispositivo se autentifique.
SIP	Protocolo de inicio de sesión. Permite sesiones de gestión de llamadas, especialmente conferencias de audio bipartitas. SIP trabaja con el Protocolo de descripción de sesión (SDP) para señalización de llamadas. Al usar SIP, el router puede admitir cualquier gateway SIP de Voz sobre IP (VoIP) y servidores de proxy VoIP.
SMTP	Protocolo simple de transferencia de correo. Un protocolo de Internet que entrega servicios de correo electrónico.
SNMP	Protocolo simple de gestión de redes. Un protocolo en redes TCP/IP que entrega un medio para monitorear y controlar dispositivos de red y administrar configuraciones, recolección de estadísticas, ejecución y seguridad.
envío basado en el origen	El envío de un paquete por un grupo de puertos basado en la dirección de origen del paquete. Contraste con el envío basado en el destino.
división de arquitectura de túneles	La división en túneles permite a los clientes VPN comunicarse en forma local sin cifrado. Los usuarios envían sólo el tráfico que está destinado a la red inicial a través del túnel. Todo el otro tráfico, como mensajería instantánea, correo electrónico o navegación casual en Internet, es enviado a Internet al usar la LAN local del cliente VPN.
SPAN	Analizador de puerto conmutado. Una función que se usa para especificar un conjunto de puertos (o VLANs) que serán monitoreados. Se envía una copia del tráfico en estos puertos de origen a un puerto de destino específico. Típicamente, un usuario conecta un network analyzer al puerto de destino para ver el tráfico en los puertos de origen. Consulte también SPAN local y SPAN remoto.
protocolo de spanning tree	Consulte STP.
dirección segura estática	Una dirección segura configurada manualmente que se almacena en la tabla de direcciones y se agrega a la configuración vigente. Consulte también dirección dinámica y dirección MAC de etiqueta.

SSH	Secure Shell. Aplicación que se ejecuta sobre un nivel de transporte confiable, como TCP/IP, que proporciona capacidades de autenticación y cifrado potentes.
SSID	Identificador de conjunto de servicios. Un código adjunto a paquetes en una red inalámbrica para identificar a cada paquete como parte de dicha red. Todos los dispositivos inalámbricos que intenten comunicarse con otros deben asociarse con el mismo SSID.
ruta estática	Una ruta que se configura explícitamente y se ingresa en una tabla de enrutamiento. Las rutas estáticas tienen preferencia sobre rutas elegidas por protocolos de enrutamiento dinámicos.
STP	Protocolo de Spanning Tree Una técnica estandarizada para mantener una red de switches o puentes múltiples. Cuando una topología de red cambia, el STP evita la creación de loops al reconfigurar de forma transparente puentes y switches y ubicar puertos en un estado de bloqueo o envío. Cada VLAN se trata como un puente separado y se aplica una instancia separada de STP a cada una.
máscara de subred	Máscara de dirección de 32-bit usada en IP para mostrar cuáles bits de una dirección IP identifican el número de red, el número de subred y el número de nodo.
puerto de switch	Una interfaz de sólo 2 capas que se asocia con un puerto físico. Puede ser un puerto de acceso o un puerto troncal.
SVI	Interfaz virtual del switch. Una VLAN con una dirección IP asignada que dispositivos de 3 capas usan para tener acceso a la VLAN. Se puede configurar un SVI para enrutar paquetes desde una VLAN a otra.

T

TCP	Protocolo TCP (Protocolo de control de transmisión). Un protocolo de capa de transporte orientado a la conexión que entrega una transmisión de datos full duplex confiable. TCP es parte de la pila de protocolo TCP/IP.
TCP/IP	El nombre común de un conjunto de protocolos que admiten la construcción de intraredes mundiales.
Telnet	Un protocolo de emulación de terminal para redes TCP/IP como Internet. Telnet es una forma común para controlar servidores de Internet en forma remota.

TFTP	Protocolo trivial de transferencia de archivos. Una versión simplificada de FTP que permite transferir archivos de un computador a otro a través de una red, usualmente sin el uso de la autentificación del cliente (por ejemplo, nombre de usuario y contraseña).
TKIP	Protocolo temporal de integridad de claves. Un cifrado que protege contra un ataque en WEP en el que el intruso utiliza un segmento de cifrado llamado vector de iniciación (VI) en paquetes cifrados para calcular la clave WEP.
puerto troncal	Un puerto que lleva el tráfico de VLANs múltiples. Contraste con el puerto de acceso.
Túnel	Canal virtual a través de un medio compartido como Internet, usado para el intercambio de paquetes de datos encapsulados.

U

UDP	Protocolo de datagrama de usuario (UDP). Un protocolo de capa de transporte sin conexión en la pila TCP/IP. UDP es un protocolo simple que intercambia datagramas sin acuse de recibo o entrega garantizada, que requiere que el procesamiento de error y la retransmisión sea gestionada por otros protocolos.
enrutamiento de unidifusión	Una técnica de enrutamiento que rutea un paquete a un destino único y usa un protocolo de enrutamiento para determinar la ruta a ese destino. Contraste con enrutamiento de multidifusión.

V

Interfaz virtual	Una interfaz que actúa como el marcador de posición del servidor DHCP para los clientes inalámbricos que obtengan su dirección IP desde un servidor DHCP y actúe como la dirección de redireccionamiento para la ventana de registro de autenticación por Internet.
VLAN	LAN virtual. Grupos de trabajo compuestos de LAN lógicos en vez de físicos agrupados por razones comerciales o para un proyecto particular, independientemente de la ubicación real de cada miembro.
VPN	red privada virtual. La misma seguridad y privacidad de red sobre una infraestructura pública que la que sería proporcionada en una red privada. VPN activan el tráfico IP para que viaje en forma segura en una red TCP/IP pública al encriptar todo el tráfico desde una red a otra. Una VPN utiliza túneles para encriptar toda la información en el nivel IP.

VTP Protocolo de enalce de VLAN. Un protocolo de mensajería de 2 capas que mantiene la consistencia de configuración de VLAN al administrar la adición, eliminación y cambio de nombre de VLANs en base a toda la red.

recorte VTP El bloqueo del tráfico de difusión inundada, de multidifusión, y de unidifusión desconocida a las VLANs en puertos troncales que están incluidos en la lista de recorte elegible.

VLAN de voz Una VLAN que es usada por un switch para tráfico de voz desde teléfonos IP. Consulte también VLAN de acceso y VLAN nativa.

W

WEP Privacidad equivalente a cableado. Un cifrado que distribuye la comunicación entre el punto de acceso y los dispositivos clientes para mantener la comunicación privada. Tanto el punto de acceso como el dispositivo cliente utilizan la misma clave WEP para cifrar y descifrar las señales de radio.

wink start El extremo de origen toma la línea al descolgar. Espera el reconocimiento desde el otro extremo antes de pulsar dígitos. Esto sirve como una verificación de integridad que identifica un enlace que funciona mal y permite que la red envíe un tono de reordenar a quien llama.

WINS Servicio de Nombres de Internet de Windows. Un sistema de Windows que determina la dirección IP asociada con una computadora de red específica.

WMM Multimedia inalámbrica. Un mejoramiento QoS para LAN inalámbricas. WMM admite dispositivos que cumplen el estándar 802.11E de QoS Basic Service Set (QBSS). WMM permite servicios diferenciados para voz, video y datos de mejor esfuerzo para permitir que el tráfico de voz antes de otro tráfico en la red.

WPA Acceso protegido por Wi-Fi. Un mejoramiento de seguridad interoperable y fundamentado en estándares que aumenta el nivel de protección de datos y el control de acceso para los sistemas de LAN inalámbricas. Por medio de la gestión de claves WPA, los clientes y el servidor de autenticación pueden autenticarse entre sí utilizando el método de autenticación EAP, y el cliente y el servidor generan una clave maestra para pares (PMK). WPA utiliza TKIP para la protección de datos y IEEE 802.1X para la gestión de claves autentificadas.

WPA2	Acceso protegido por Wi-Fi 2. Un mejoramiento de seguridad interoperable y fundamentado en estándares que utiliza AES CCMP para la protección de datos. WPA2 ofrece un mayor nivel de seguridad que WPA porque AES ofrece un cifrado más fuerte que TKIP.
WPA-PSK	Clave previamente compartida para acceso protegido por Wi-Fi. Un método de autenticación que admite WPA en una LAN inalámbrica donde no está disponible la autenticación con base IEEE 802.1X. Una clave previamente compartida se configura tanto en el cliente como en el punto de acceso.
WPA2-PSK	Clave previamente compartida para acceso protegido por Wi-Fi 2. Un método de autentificación que admite WPA2 en una LAN inalámbrica donde no está disponible la autentificación con base IEEE 802.1X. Una clave previamente compartida se configura tanto en el cliente como en el punto de acceso.