

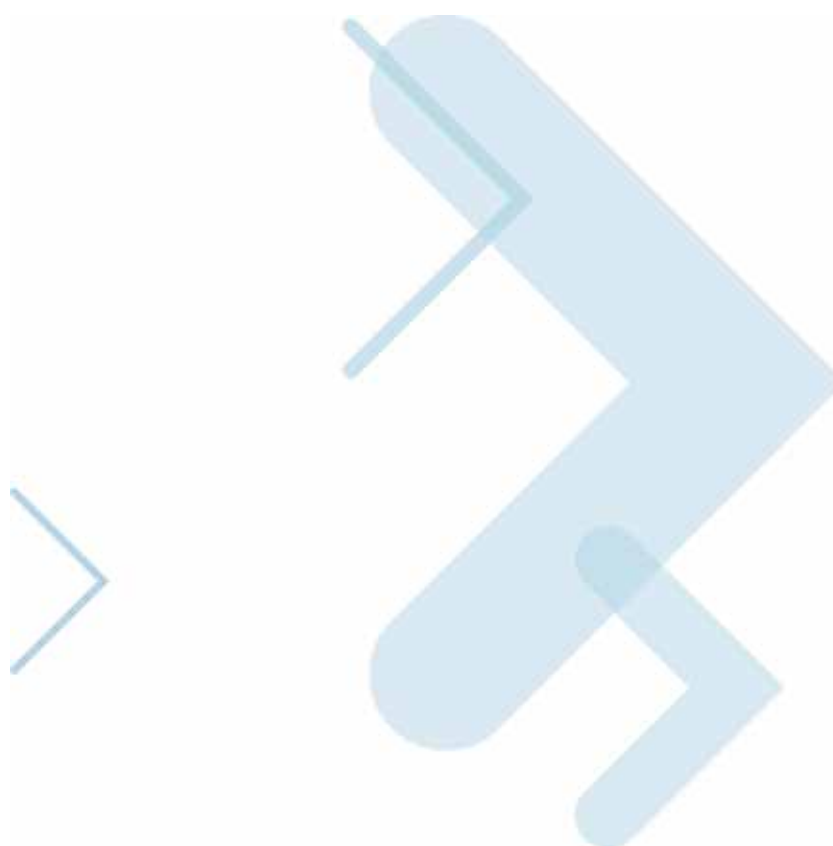


Motorola SURFboard[®]

Puerta de enlace de voz inalámbrica serie
SVG1501

Guía del usuario

*SVG1501
SVG1501E
SVG1501U
SVG1501UE



© 2009 Motorola, Inc. Todos los derechos reservados. No se puede reproducir ninguna parte de esta publicación de ninguna forma, por ningún medio, ni se puede utilizar para realizar ningún trabajo derivado (como traducción, transformación o adaptación) sin autorización por escrito de Motorola, Inc.

MOTOROLA y el logotipo de la M estilizada están registrados en la Oficina de Patentes y Marcas Comerciales de los EE.UU. SURFboard es una marca comercial registrada de General Instrument Corporation, una subsidiaria que pertenece totalmente a Motorola, Inc. Microsoft, Windows, Windows NT, Windows Vista, Internet Explorer, DirectX y Xbox LIVE son marcas comerciales registradas de Microsoft Corporation; y Windows XP es una marca comercial de Microsoft Corporation. Linux® es una marca comercial registrada de Linus Torvalds en los Estados Unidos y en otros países. UNIX es una marca comercial registrada de The Open Group en los Estados Unidos y en otros países. Macintosh es una marca comercial registrada de Apple Computer, Inc. Adobe, Adobe Acrobat y Adobe Acrobat Reader son marcas comerciales registradas de Adobe Systems, Inc. Todos los otros nombres de productos o servicios son propiedad de sus respectivos dueños. No se puede reproducir ni transmitir ninguna parte de este documento de ninguna forma y por ningún medio sin la autorización por escrito de la editorial.

Motorola se reserva el derecho de revisar esta publicación y de realizar cambios en el contenido eventualmente sin obligación por parte de Motorola de proporcionar notificación de dicha revisión o cambio. Motorola proporciona esta guía sin garantía de ningún tipo, implícita o explícita, incluidas pero no limitadas a las garantías implícitas de comerciabilidad e idoneidad para un propósito en particular. Motorola pueden realizar mejoras o cambios en los productos descriptos en este manual en cualquier momento.



Información sobre seguridad y reglamentaciones

INSTRUCCIONES IMPORTANTES DE SEGURIDAD

Cuando use su equipo telefónico, siempre siga las precauciones de seguridad básicas para reducir el riesgo de incendio, descarga eléctrica y daños a las personas, entre ellas:

- Lea todas las instrucciones detalladas aquí y/o en el manual del usuario antes de usar este dispositivo. Preste especial atención a todas las precauciones de seguridad. Conserve las instrucciones para referencia en el futuro.
- Este dispositivo se debe instalar y utilizar siguiendo estrictamente las instrucciones del fabricante, como se describen en la documentación del usuario que se incluye con el dispositivo.
- Cumpla todas las notificaciones de advertencia y precaución proporcionadas en las instrucciones. Observe todos los símbolos de advertencia y precaución indicados en este dispositivo.
- Para evitar riesgo de incendio o descarga, no exponga el dispositivo a la lluvia o humedad. Este dispositivo no se debe mojar ni salpicarse. No coloque objetos llenos de líquido, como floreros, sobre el dispositivo.
- Este dispositivo fue calificado bajo condiciones de prueba, incluido el uso de los cables suministrados entre los componentes del sistema. Para garantizar el cumplimiento reglamentario y de seguridad, use únicamente los cables de alimentación e interfaz suministrados e instálelos correctamente.
- Se pueden utilizar diferentes tipos de cables conectores para las conexiones al circuito de suministro principal. Use únicamente un cable de línea principal que cumpla con todos los requisitos de seguridad del dispositivo aplicables en el país de uso.
- La instalación debe realizarse conforme a los códigos de cableado nacional y a las reglamentaciones locales.
- Use este dispositivo únicamente desde el tipo de fuente de alimentación indicado en la etiqueta señalizadora del dispositivo. Si no está seguro del tipo de alimentación de su hogar, consulte a su representante o empresa local de energía.
- No sobrecargue los tomacorrientes ni los cables de extensión, dado que pueden causar riesgo de incendio o descarga eléctrica. Los tomacorrientes de CA o los cables de extensión sobrecargados, los cables de alimentación raídos, el aislamiento de cables dañado o rajado, y los enchufes rotos son peligrosos. Pueden provocar riesgo de incendio o descarga.
- Coloque los cables de la fuente de alimentación en canales para que no haya posibilidad de que los pisen o que sean comprimidos por elementos colocados encima o contra ellos. Preste especial atención a la unión de los cables con los enchufes y los receptáculos de conveniencia, y examine el punto donde salen del dispositivo.
- Coloque este dispositivo en una ubicación que esté lo suficientemente cerca de un tomacorriente y se adecue a la longitud del cable de alimentación.

- Ubique el dispositivo para permitir el fácil acceso cuando se desconecte el cable de alimentación del dispositivo del tomacorriente de CA.
- No conecte el enchufe en un cable de extensión, receptáculo u otra salida a menos que el enchufe pueda insertarse completamente sin que ninguna parte de las clavijas quede expuesta.
- Ubique este dispositivo en una superficie estable.
- Se recomienda que el cliente instale un protector de sobretensiones de CA en el tomacorriente de CA al que se conecta este dispositivo. Esto es para evitar que rayos locales y otras sobretensiones eléctricas dañen el dispositivo.
- Postergue la instalación hasta que no haya riesgo de tormenta eléctrica o rayos en el área.
- Evite usar un teléfono (que no sea de tipo inalámbrico) durante una tormenta eléctrica. Puede existir riesgo de descarga eléctrica de los rayos. Para mayor protección, desenchufe el dispositivo del tomacorriente y desconecte los cables para evitar daño en el dispositivo a causa de rayos y sobrecarga de energía.
- Este producto es para uso en interiores exclusivamente. No coloque el cable telefónico o de Ethernet fuera del edificio. Si los rayos entran en contacto con los cables, puede ocasionarse un riesgo de seguridad y el producto puede dañarse.
- No cubra el dispositivo ni bloquee el flujo de aire del dispositivo con ningún otro objeto. Aleje el dispositivo de la humedad, el calor excesivo, la vibración y el polvo.
- Use solamente el cable de alimentación y las baterías indicadas en este manual. No incinere las baterías. Pueden explotar. Consulte los códigos locales para obtener posibles instrucciones especiales sobre la manera de desecharlas.
- Limpie el dispositivo con un paño seco y limpio. Nunca use líquidos limpiadores o químicos similares. No rocíe limpiadores directamente sobre el dispositivo ni use aire a presión para quitar el polvo.
- **PRECAUCIÓN:** Para reducir el riesgo de incendio, use únicamente el calibre de alambre estadounidense (AWG) N° 26 o superior (por ejemplo, 24 AWG) clasificación UL, o el cable de línea de telecomunicaciones certificado por la Asociación de Normas Canadiense (CSA), o el equivalente nacional.
- Desconecte los conectores de circuito de voltaje de red de telecomunicación (TNV) antes de cortar la electricidad.
- Desconecte el conector del circuito TNV antes de quitar la cubierta.
- No use este producto cerca del agua: por ejemplo, cerca de una bañera, lavabo, fregadero o tina del lavadero, en un sótano húmedo o cerca de una piscina.
- No use el teléfono cerca de una fuga de gas para informar esta situación.
- Al finalizar cualquier servicio de mantenimiento o reparación de este dispositivo, solicite al técnico de servicio que realice las verificaciones de seguridad para determinar que el dispositivo esté funcionando de manera segura.
- No abra el dispositivo. No realice ningún servicio de mantenimiento que no sean los contenidos en las instrucciones de instalación y solución de problemas. Consulte todos los servicios de mantenimiento con el personal de servicio calificado.
- Este dispositivo no se debe utilizar en un ambiente que supere los 40° C.

CONSERVE ESTAS INSTRUCCIONES

Nota para el instalador del sistema de CATV: Este recordatorio se suministra para advertir al instalador del servicio de televisión por cable (CATV) de la Sección 820.93 del Código Eléctrico Nacional, que proporciona las directivas para la correcta descarga a tierra y, en especial, especifica que la cubierta protectora del cable coaxial debe estar conectado al sistema de descarga a tierra del edificio, lo más cercano al punto de entrada del cable que sea factible.

CUIDADO DEL MEDIO AMBIENTE A TRAVÉS DEL RECICLADO



Cuando vea este símbolo en un producto Motorola, no deseche el producto con los desperdicios domésticos o comerciales.

Reciclado de su equipo Motorola

No deseche este producto con los desperdicios domésticos o comerciales. Algunos países o regiones, como la Unión Europea, han organizado sistemas de recolección y reciclado de desechos eléctricos y electrónicos. Comuníquese con las autoridades locales para obtener información sobre las prácticas establecidas en su región. Si los sistemas de recolección no se encuentran disponibles, llame al Servicio al cliente de Motorola para obtener ayuda. Visite www.motorola.com/recycle para obtener instrucciones sobre el reciclado.

INFORMACIÓN IMPORTANTE SOBRE EL SERVICIO DE VOZ POR INTERNET



Comuníquese con su proveedor de servicios de Internet (ISP) y/o con el municipio local para obtener información adicional sobre cómo realizar llamadas de emergencia usando el servicio de voz por Internet (VoIP) en su área.

Cuando use este dispositivo de voz por Internet, NO PUEDE realizar ninguna llamada, incluidas las llamadas de emergencia. Los servicios de ubicación E911 NO ESTARÁN disponibles dadas las siguientes circunstancias:

- Su conexión ISP de banda ancha está fuera de servicio, se corta o falla de otra manera.
- Se corta la corriente eléctrica.

Cuando use este dispositivo VoIP, puede realizar una llamada de emergencia a un operador, pero los servicios de ubicación E911 no estarán disponibles dadas las siguientes circunstancias:

- Ha cambiado la dirección física de su dispositivo VoIP, y no realizó la actualización o el aviso de este cambio a su proveedor de servicio VoIP.
- Está usando un número de teléfono que no pertenece a los Estados Unidos.
- La base de datos de información de ubicación automática local presenta demoras para poner a disposición la información de su ubicación.

Nota: Su proveedor de servicios, no Motorola, es responsable del abastecimiento de los servicios de telefonía VoIP a través de este equipo. Motorola no será responsable por ninguna eventualidad directa o indirecta, daños, pérdidas, reclamos, demandas, medidas, causas de acciones, riesgos o peligros derivados de los servicios suministrados a través de este equipo o relacionados con ellos, y no los reconoce expresamente.

DECLARACIONES DE LA COMISIÓN FEDERAL DE COMUNICACIONES

DECLARACIÓN DE INTERFERENCIA CON LA COMISIÓN FEDERAL DE COMUNICACIONES

Este equipo ha sido probado y se ha determinado que cumple con los límites para un dispositivo digital de Clase B según el Apartado 15 de las normas de la Comisión Federal de Comunicaciones (FCC). Estos límites están diseñados para proveer protección razonable contra interferencias perjudiciales en un ambiente residencial. Este equipo genera, utiliza y puede irradiar energía de radiofrecuencia y, si no se instala y utiliza de acuerdo con las instrucciones, puede causar interferencias perjudiciales a las radiocomunicaciones. No obstante, no hay garantía de que no se produzcan interferencias en alguna instalación en particular. Si el equipo causa interferencia perjudicial a la recepción de radio o televisión, lo que puede determinarse al encender y apagar el dispositivo, se recomienda que el usuario trate de corregirla mediante una o más de las siguientes medidas:

- Reorientar o reubicar la antena.
- Aumentar la separación entre el dispositivo y el receptor.
- Conectar el equipo a una salida de alimentación de un circuito diferente de aquél al que está conectado el receptor.
- Consultar con el distribuidor o solicitar ayuda de un técnico de radio/TV con experiencia.

Este dispositivo cumple con las normas del Apartado 15 de la FCC. La operación está sujeta a las dos condiciones siguientes: (1) este dispositivo no puede causar interferencias perjudiciales y (2) este dispositivo debe aceptar cualquier interferencia recibida, incluida la interferencia que puede causar la operación involuntaria.

PRECAUCIÓN DE LA COMISIÓN FEDERAL DE COMUNICACIONES: Cualquier cambio o modificación no aprobada expresamente por Motorola en referencia al cumplimiento podría anular la autoridad del usuario para operar el equipo.

DECLARACIÓN SOBRE EXPOSICIÓN DE RADIACIÓN DE LA COMISIÓN FEDERAL DE COMUNICACIONES

Este equipo cumple con los límites de exposición de radiación de la FCC establecidos para un ambiente no controlado. Para cumplir con los requisitos de cumplimiento de exposición de radiofrecuencia de la FCC, la separación entre la antena y el cuerpo de cualquier persona (incluidas manos, muñecas, pies y tobillos) debe ser de por lo menos 20 cm (8 pulgadas).

Este transmisor no debe ubicarse o funcionar junto a cualquier otra antena o transmisor.

La disponibilidad de algunos canales y/o bandas de frecuencia operativa específicos dependen del país y están programados de fábrica en el firmware para que coincidan con los destinos previstos. El usuario final no puede acceder a la configuración de firmware.

DECLARACIÓN SOBRE LA INDUSTRIA CANADIENSE

Este dispositivo cumple con las normas RSS-210 de la Industria Canadiense (IC).

La operación está sujeta a las dos condiciones siguientes:

- este dispositivo no puede causar interferencia y
- este dispositivo debe aceptar cualquier interferencia, incluida la interferencia que puede causar la operación involuntaria del dispositivo.

Este aparato digital de Clase B cumple con las normas canadienses ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

DECLARACIÓN SOBRE EXPOSICIÓN DE RADIACIÓN DE LA INDUSTRIA CANADIENSE

NOTA IMPORTANTE: Este equipo cumple con los límites de exposición de radiación de la IC establecidos para un ambiente no controlado. Este equipo se debe instalar y utilizar con una distancia mínima de 20 cm entre el radiador y su cuerpo.

INFORMACIÓN DE LA RED LAN INALÁMBRICA

Este dispositivo es un producto de red inalámbrico que usa las tecnologías de radio Espectro Ensanchado por Secuencia Directa (DSSS) y Acceso Múltiple por División de Frecuencias Ortogonales (OFDMA). El dispositivo está diseñado para interactuar con cualquier otro producto DSSS y OFDMA que cumpla con:

- El estándar IEEE 802.11 sobre redes LAN inalámbricas (Revisión B y Revisión G), según define y aprueba el Instituto de Ingenieros Eléctricos y Electrónicos
- La certificación de fidelidad inalámbrica (Wi-Fi) según define la Alianza de Compatibilidad de Ethernet Inalámbrica (WECA).



RESTRICCIONES EN EL USO DE LOS DISPOSITIVOS INALÁMBRICOS

En algunas situaciones o ambientes, el uso de dispositivos inalámbricos puede ser restringido por el dueño del edificio o los representantes responsables de la organización. Por ejemplo, el uso de un equipo inalámbrico en cualquier ambiente en el que el riesgo de interferencia con otros dispositivos o servicios se percibe o identifica como perjudicial.

Si no está seguro de las políticas que se aplican al uso de equipos inalámbricos en una organización y ambiente específicos, se recomienda que solicite autorización para el uso del dispositivo antes de encender el equipo.

El fabricante no es responsable de ninguna interferencia de radio o televisión causada por la modificación no autorizada de los dispositivos incluidos con este producto, o la sustitución o fijación de cables de conexión y equipos que no sean los especificados por el fabricante. La corrección de la interferencia causada por dicha modificación, sustitución o fijación no autorizada es responsabilidad del usuario.

El fabricante y sus revendedores o distribuidores autorizados no son responsables de ningún daño o violación a las reglamentaciones gubernamentales que pueda resultar del no cumplimiento de estas directivas.

ADVERTENCIA DE SEGURIDAD: Este dispositivo le permite crear una red inalámbrica. Los usuarios no autorizados podrían obtener acceso a las conexiones de red inalámbricas. Para obtener más información sobre cómo proteger su red, consulte [Configuración de su red LAN inalámbrica](#) o visite el sitio Web de Motorola.

DECLARACIÓN INTERNACIONAL DE CONFORMIDAD

Nosotros, Motorola, Inc., 101 Tournament Drive, Horsham, PA 19044, Estados Unidos, declaramos bajo nuestra exclusiva responsabilidad que la puerta de enlace de voz serie SURFboard SVG1501 a la que se relaciona esta declaración concuerda con uno o más de los siguientes estándares:

EN60950-1 EN 300 328 EN 301 489-1/-17

EN61000-3-2 EN61000-3-3

Disposiciones de las Directivas del Consejo de la Unión Europea:

- Directiva de compatibilidad electromagnética (EMC) 2004/108/EC
- Directiva de bajo voltaje 2006/95/EC
- Equipos radioeléctricos y equipos terminales de telecomunicación (R&TTE) 1999/5/EC
- Directiva de residuos de aparatos eléctricos y electrónicos (WEEE) 2002/96/EC
- Directiva de restricción del uso de determinadas sustancias perjudiciales en equipos eléctricos (RoHS) 2002/95/EC

Índice

Información sobre seguridad y reglamentaciones

Descripción general

Información del contacto	1
Funciones estándar	1
Opciones de red LAN para la unidad SVG1501	2
Conexión USB (únicamente SVG1501U)	2
Red LAN inalámbrica.....	3
Red LAN Ethernet cableada.....	4
Panel frontal.....	5
Panel posterior.....	6
Etiqueta de control de acceso de medios	7

Información general

Dentro de la caja.....	8
Antes de comenzar.....	9
Inicio de sesión de servicio	9
Requisitos del sistema	9
Conexión de la unidad SVG1501	10
Conexión de la unidad SVG1501U.....	12
Instalación en pared de la unidad SVG1501	13
Plantilla para la instalación en pared.....	15
Configuración del acceso a Internet	16
Configuración de TCP/IP en Windows XP.....	16
Configuración de TCP/IP en Windows Vista.....	16
Verificación de la dirección IP en Windows XP.....	17
Verificación de la dirección IP en Windows Vista	17
Renovación de su dirección IP	18
Configuración de una red Wi-Fi	18

Configuración básica

Inicio del administrador de configuración (CMGR) de la unidad SVG1501.....	19
Barra del menú Opciones de la unidad SVG1501.....	20
Obtención de ayuda.....	21
Cómo salir del administrador de configuración de la unidad SVG1501	21

Páginas de estado

Página de estado del software	22
Página de estado de la conexión	22
Página de estado de la seguridad.....	23
Cambio de la contraseña predeterminada de la unidad SVG1501	23
Restauración los valores predeterminados de fábrica	24
Página de estado del diagnóstico	24

Herramienta Ping	24
Herramienta Encaminamiento de rastreo	26
Página de estado del registro de eventos	27
Páginas básicas	
Página básica de configuración.....	28
Página básica del protocolo DHCP	30
Página básica de DDNS	32
Página básica de copia de seguridad	33
Restauración de la configuración de su unidad SVG1501	33
Copia de seguridad de la configuración de su unidad SVG1501	33
Páginas avanzadas	
Página avanzada de opciones	34
Página avanzada de filtrado de IP	36
Página avanzada de filtrado de MAC	37
Configuración de un filtro de dirección MAC	37
Página avanzada de filtrado de puerto	38
Página avanzada de redireccionamiento de puertos	39
Página avanzada de disparadores de puertos	40
Página avanzada de host de DMZ	41
Configuración del host de DMZ	42
Página avanzada del protocolo de información de enrutamiento	42
Páginas de firewall	
Página de filtrado del contenido Web del firewall	44
Página de registro local del firewall	45
Página de registro local del firewall	45
Páginas de control para padres	
Página de configuración del usuario del control para padres	47
Página de configuración básica del control para padres	49
Página de filtrado de hora del día del control para padres	50
Página del registro local del control para padres	50
Páginas inalámbricas	
Página de radio inalámbrico 802.11	51
Página de red principal inalámbrica 802.11	52
Página avanzada inalámbrica 802.11	54
Página de control del acceso inalámbrico 802.11	56
Página de multimedia inalámbrica 802.11	57
Página de extensión inalámbrica 802.11	58
Configuración de su red LAN inalámbrica	59
Cifrado de las transmisiones de la red LAN inalámbrica	59
Instalación de clientes inalámbricos	60
Instalación de un cliente inalámbrico para WPA	61
Configuración de un cliente inalámbrico para WEP	61

Configuración de un cliente inalámbrico con el nombre de la red (SSID)	61
Páginas de VPN	
Página básica de VPN	62
Página IPsec de VPN	63
Página L2TP/PPTP de VPN.....	67
Página del registro de eventos de VPN.....	68
Páginas de MTA	
Página de estado de MTA	69
Página de DHCP de MTA	69
Página de QoS de MTA	70
Página de suministro de MTA	70
Página del registro de eventos de MTA	71
Solución de problemas	
Soluciones	72
Indicadores LED del panel frontal y condiciones de error	73
Licencia de software	

1

Descripción general

La unidad de voz inalámbrica Motorola SURFboard® SVG1501 se puede utilizar en hogares con uno o más equipos con capacidad de conexión inalámbrica para acceso remoto a la puerta de enlace de voz inalámbrica.

Esta guía del usuario brinda una descripción general del producto e información de configuración para la unidad SVG1501. Además proporciona instrucciones para la instalación de la puerta de enlace de voz inalámbrica y configuración de la red LAN inalámbrica, Ethernet, enrutador, protocolo de control dinámico de host (DHCP) y ajustes de seguridad.

Nota: Todas las referencias sobre la unidad SVG1501 utilizadas en esta guía también se aplican a las unidades SVG1501U, SVG1501E y SVG1501UE, a menos que se indique lo contrario. Todas las referencias sobre la unidad SVG1501U también se aplican a la unidad SVG1501UE.

Información del contacto

- Si tiene alguna pregunta o necesita ayuda con la puerta de enlace de voz inalámbrica SVG1501, comuníquese con su proveedor de servicios de Internet.
- Para obtener información sobre el servicio al cliente, soporte técnico o reclamos de garantía, consulte la tarjeta de información reglamentaria, de seguridad, garantía y licencia de software de la unidad SVG1501 provista con la puerta de enlace de voz inalámbrica SVG1501.

Funciones estándar

La puerta de enlace de voz inalámbrica SVG1501 ofrece las siguientes funciones:

- Combinación de cinco productos diferentes en una unidad compacta: un cable módem DOCSIS® 2.0, un punto de acceso inalámbrico IEEE 802.11g (Wi-Fi® certificado), conexiones Ethernet 10/100Base-T, dos conexiones de teléfono por Internet VoIP y firewall.
- Firewall mejorado para mayor seguridad de red contra ataques no deseados a través de Internet. Compatibilidad con inspección de estado, detección de intrusiones, zona desmilitarizada (DMZ), prevención del ataque de negación de servicio y traducción de dirección de red (NAT).
- Cifrado de datos y control del acceso a redes para las transmisiones inalámbricas
- Asistente para instalación inalámbrica y configuración de seguridad fáciles

- Cable módem de alta velocidad integrado para acceso continuo de banda ancha
- Una conexión de banda ancha para hasta 245 equipos
- Acceso inalámbrico IEEE 802.11g para redes hogareñas o pequeñas
- Servicio telefónico del protocolo de voz por Internet (VoIP) con dos líneas telefónicas
- Conexión de banda ancha segura con fidelidad inalámbrica (Wi-Fi) para dispositivos habilitados para Wi-Fi
- Cuatro puertos de enlace ascendente Ethernet 10/100Base-T compatibles con conexiones bidireccionales no simultáneas o bidireccionales simultáneas con capacidad de interfaz automática cruzada dependiente del medio (MDIX)
- Conexión de bus universal en serie (USB) para un sólo equipo (únicamente modelos SVG1501U)
- Enrutamiento para una red LAN inalámbrica (WLAN) o una red LAN Ethernet cableada
- Servidor DHCP integrado para configurar una red LAN privada Clase C cableada y/o inalámbrica combinada
- Operación de transferencia de red privada virtual (VPN) compatible con IPSec, PPTP o L2TP para conectar de forma segura equipos remotos a través de Internet.
- Administrador de configuración (CMGR) SVG1501 que ofrece fácil configuración de los ajustes inalámbricos, de seguridad, Ethernet, DHCP y del enrutador
- Compatibilidad con fax y módem telefónico
- Servicio telefónico de VoIP a través de su conexión de cable que ofrece muchos servicios telefónicos tradicionales como:
 - Llamadas locales y de larga distancia
 - Llamadas tripartitas
 - Correo de voz
 - Remarcación de números
 - Marcaciones rápidas
 - Identificador de llamadas, llamada en espera, transferencia de llamadas, devolución de llamadas

Opciones de red LAN para la unidad SVG1501

Puede conectar hasta 245 equipos cliente a la unidad SVG1501 usando una o más combinaciones de las siguientes conexiones de red:

- Bus universal en serie (USB) – únicamente modelos SVG1501U
- Red LAN inalámbrica (WLAN)
- Red de área local (LAN) Ethernet
- Conexiones Wi-Fi para dispositivos habilitados para Wi-Fi

Conexión USB (únicamente SVG1501U)

Puede conectar un único equipo que ejecute Windows XP o Windows Vista al puerto USB V2.0 de la unidad SVG1501U.

Red LAN inalámbrica

Una red inalámbrica elimina la necesidad de cableado para conectar equipos en el hogar o la oficina. Cada equipo o dispositivo en una red WLAN debe estar habilitado para Wi-Fi con un adaptador inalámbrico externo o integrado.

Computadoras portátiles: Use un adaptador de computadora portátil inalámbrico integrado, un adaptador de ranura PCMCIA inalámbrico o un adaptador USB inalámbrico.

Computadoras de escritorio: Use un adaptador PCI inalámbrico, un adaptador USB inalámbrico o un producto compatible en la ranura PCI o puerto USB, respectivamente.



Ejemplo de conexiones de red inalámbricas (modelo SVG1501U mostrado)

Para configurar la unidad SVG1501 en un equipo cableado a la unidad SVG1501 con una conexión Ethernet, lleve a cabo los procedimientos detallados en la sección **Páginas inalámbricas**. No intente configurar la unidad SVG1501 a través de una conexión inalámbrica.

La distancia máxima de funcionamiento inalámbrico depende del tipo de materiales a través de los cuales la señal debe atravesar, la ubicación de su unidad SVG1501 y los clientes (estaciones). Motorola no puede garantizar el funcionamiento inalámbrico para todas las distancias compatibles en todos los ambientes.

Red LAN Ethernet cableada

Puede conectar cualquier PC con un puerto LAN Ethernet a la conexión Ethernet de la unidad SVG1501. Dado que el puerto Ethernet de la unidad SVG1501 es compatible con la interfaz MDIX automática, puede utilizar un cable recto o cruzado para conectar un concentrador, conmutador o equipo. Utilice cables de Categoría 5, o superior, para todas las conexiones Ethernet.



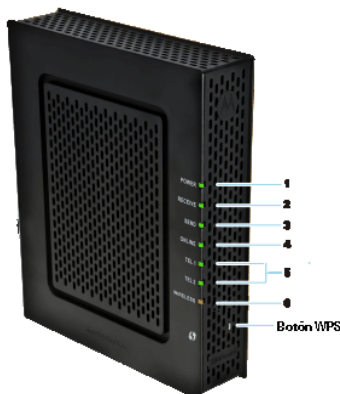
Ejemplo de conexión Ethernet a equipo (modelo SVG1501U mostrado)

Una red LAN Ethernet cableada con más de cuatro equipos requiere uno o más concentradores, conmutadores o enrutadores. Puede:

- Conectar un concentrador o conmutador a cualquier puerto Ethernet en la unidad SVG1501.
- Usar concentradores, conmutadores o enrutadores Ethernet para conectar cualquier combinación de hasta 245 equipos y clientes inalámbricos a la unidad SVG1501.

Panel frontal

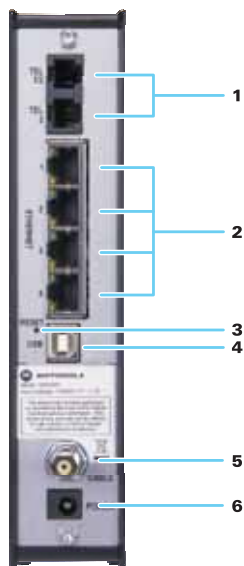
El panel frontal de la unidad SVG1501 contiene luces indicadoras y el **botón WPS** que se utiliza para configurar la seguridad de Wi-Fi protegida (WPS) en los clientes compatibles conectados a la red SVG1501.



Los indicadores LED del panel frontal de la unidad SVG1501 brindan la siguiente información de estado referida al encendido, comunicaciones y errores:

LED	Destello	Encendido
1 POWER (ENCENDIDO)	No se aplica. El indicador LED no destella.	Verde: La energía está conectada correctamente.
2 RECEIVE (RECIBIR)	Está buscando una conexión de canal receptor.	Verde: El canal receptor está conectado.
3 SEND (ENVIAR)	Está buscando una conexión de canal emisor.	Verde: El canal emisor está conectado.
4 ONLINE (EN LÍNEA)	Está buscando una conexión de Internet, transmitiendo o recibiendo datos a través de Internet.	Verde: El proceso de arranque se ha completado.
5 TEL1 TEL 2	El teléfono está descolgado, marcando o con una llamada en curso.	Verde: El teléfono está conectado, activado y disponible.
6 WIRELESS (INALÁMBRICO)	Verde: Está habilitado para Wi-Fi con actividad inalámbrica de datos cifrados. Los destellos largos/cortos indican emparejamiento inalámbrico con la tarjeta cliente en curso. Ámbar: Está habilitado para Wi-Fi con actividad inalámbrica de datos no cifrados.	Verde: Se estableció con éxito el emparejamiento inalámbrico entre la unidad SVG1501 y otro dispositivo habilitado para Wi-Fi en su red: teléfono celular, asistente digital personal (PDA), computadora portátil, etc. Ámbar: Se estableció con éxito el emparejamiento móvil. La luz cambia a verde después de cinco minutos.

Panel posterior



Los paneles posteriores de la unidad SVG1501 y la unidad SVG1501U (mostrados arriba) contienen los siguientes conectores y puertos de cableado:

Elemento	Descripción
1 TEL1/2 TEL 2	Conexión de VoIP para un teléfono de una o dos líneas Conexión de VoIP para un teléfono de una línea
2 ETHERNET 1 2 3 4	Use cualquier puerto Ethernet para conectar un equipo, concentrador, puente o conmutador equipado con Ethernet usando un cable RJ-45. LED de actividad: El indicador LED verde define la actividad del conector de Ethernet. Cuando el indicador LED está encendido, no hay tráfico de datos y la conexión está estabilizada. Cuando el indicador LED está destellando, se están transmitiendo (enviando o recibiendo) datos. Cuando el indicador LED está apagado, la unidad no está encendida o no hay conexión Ethernet. LED de 10/100: Indica la tasa de transmisión de datos de la conexión. Cuando el indicador LED verde está encendido, la tasa de la conexión es de 100Base-T. Cuando el indicador LED ámbar está encendido, la tasa de la conexión es de 10Base-T.

Elemento	Descripción
3 RESET (REINICIO)	<p>Reinicia la puerta de enlace de voz inalámbrica. Puede demorar de cinco a 30 minutos para encontrar y acoplarse a los canales de comunicación apropiados.</p> <p>Mantenga presionado el botón RESET (REINICIO) durante cinco segundos o más para restaurar la configuración predeterminada de fábrica.</p>
4 USB	<p>Para Windows únicamente, puede usar el puerto USB para conectar un equipo PC a la unidad SVG1501U. No puede conectar un equipo Macintosh o UNIX® al puerto USB en la unidad SVG1501U.</p> <p>Nota: El conector USB está disponible únicamente en los modelos SVG1501U.</p>
5 CABLE	Conecta la unidad SVG1501 a un tomacorriente de cable.
6 POWER (ENCENDIDO)	Suministra energía a la unidad SVG1501.

Etiqueta de control de acceso de medios

La etiqueta de control de acceso de medios (MAC) de la unidad SVG1501, ubicada en la parte inferior de la unidad SVG1501, contiene un valor único de 48 bits que identifica cada dispositivo de red Ethernet. Para recibir servicio de datos, deberá suministrar la dirección MAC marcada como **HFC MAC ID** a su proveedor de servicios de Internet. Para recibir el servicio de VoIP, debe suministrar la identificación **MTA MAC ID** a su proveedor de VoIP.








2

Información general

Dentro de la caja

Verifique que los siguientes elementos estén incluidos en la caja con la unidad SVG1501:

Elemento		Descripción
Cable de alimentación		Conecta la unidad SVG1501 a un tomacorriente de CA.
Cable de Ethernet 10/100Base-T		Conecta la unidad SVG1501 a la red a través del puerto Ethernet. El cable debe ser Cat 5 estándar o superior.
Licencia de software y tarjeta de reglamentaciones		Contiene la licencia de software, garantía e información de seguridad de la unidad SVG1501.
CD-ROM de instalación de SVG1501		Contiene el asistente de Wi-Fi, el contrato de licencia de software, Guías del usuario de la unidad SVG1501 en varios idiomas y controladores USB de la unidad SVG1501 (únicamente modelos SVG1501U).
Hoja de instalación de SVG1501		Brinda información básica para configuración de la unidad SVG1501.

Necesitará un cable coaxial de 75-ohm con conectores de tipo F para conectar la unidad SVG1501 a la salida de cable más cercana. Si hay un TV conectado a la salida de cable, es posible que necesite un bifurcador de radiofrecuencia de 5 a 900 MHz y dos cables coaxiales adicionales para usar el TV y la unidad SVG1501.

Antes de comenzar

Tome las siguientes precauciones antes de instalar la unidad SVG1501:

- Espere hasta que no haya riesgo de tormenta eléctrica o rayos en el área.
- Para evitar descargas potenciales, siempre desenchufe el cable de alimentación del tomacorriente u otra fuente de alimentación antes de desconectarlo del panel posterior de la unidad SVG1501.
- Para evitar el recalentamiento de la unidad SVG1501, no bloquee los orificios de ventilación situados a los costados de la unidad. No abra la unidad. Remita todos los servicios de mantenimiento a su proveedor de servicios de Internet.
- No conecte los cables Ethernet y USB al mismo equipo. Conecte el cable Ethernet o el cable USB.

Verifique que tenga los cables, adaptadores y software adaptador requeridos. Verifique que los controladores correctos estén instalados para el adaptador de Ethernet en cada equipo conectado a la red. Para obtener más información sobre la configuración de la red WLAN, consulte [Configuración inalámbrica de su red LAN](#).

Inicio de sesión de servicio

Debe iniciar sesión con un proveedor de servicios de Internet para obtener acceso a Internet y otros servicios en línea.

- Para obtener el servicio de datos, deberá suministrar la dirección MAC marcada como **HFC MAC ID** que se encuentra impresa en la [Etiqueta MAC](#).

Requisitos del sistema

Su equipo debe cumplir con los siguientes requisitos mínimos:

- Computadora con procesador Pentium® o superior
- Sistema operativo Windows XP, Windows Vista, Macintosh o UNIX con el CD-ROM del sistema operativo disponible
- Cualquier explorador Web, como Microsoft Internet Explorer, Netscape Navigator® o Mozilla® Firefox®

Conexión de la unidad SVG1501

PRECAUCIÓN: Para reducir el riesgo de incendio, use únicamente un cable N° 26 o superior clasificación UL, o un cable de línea de telecomunicaciones certificado por la Asociación de Normas Canadienses (CSA), o el equivalente nacional para conectar una línea telefónica a su unidad SVG1501.

Comuníquese con su proveedor de servicios antes de conectar su unidad Motorola SVG1501 a su cableado telefónico existente. No conecte el cable de teléfono a un servicio telefónico tradicional (PSTN).

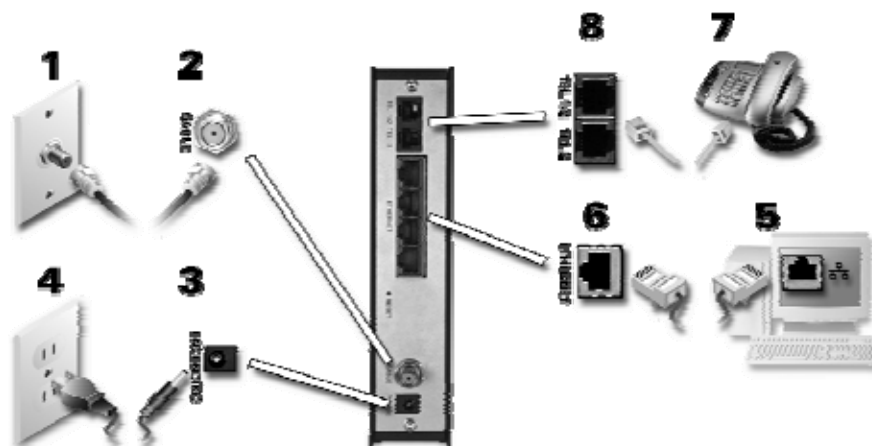
Antes de comenzar, asegúrese de que el equipo esté encendido y que el cable de alimentación de la unidad SVG1501 esté enchufado.

1. Conecte el cable coaxial al bifurcador o a la salida de cable y luego al conector de cable en la unidad SVG1501. Ajuste manualmente los conectores para evitar dañarlos.
2. Enchufe el cable de alimentación al puerto de encendido en la unidad SVG1501 y luego a un tomacorriente eléctrico.

Esto enciende automáticamente la puerta de enlace. No necesita desenchufar la puerta de enlace cuando no está en uso. La primera vez que enchufe la unidad SVG1501, demorará de cinco a 30 minutos en encontrar y acoplarse a los canales de comunicación apropiados.

3. Conecte el cable Ethernet al puerto Ethernet en el equipo y luego al puerto Ethernet en la puerta de enlace.
4. Conecte el cable telefónico de un teléfono de una o dos líneas al teléfono y luego al puerto TEL 1/2 en la parte posterior de la unidad SVG1501.

Nota: Comuníquese con un proveedor de servicios de VoIP para activar este servicio.



5. Para un segundo teléfono, conecte el cable telefónico de un teléfono de una línea al puerto TEL 2 en la parte posterior de la unidad SVG1501.
6. Verifique que los indicadores LED en el panel frontal atraviesen la siguiente secuencia:

Actividad del LED de la unidad SVG1501 durante el arranque

LED	Descripción
POWER (ENCENDIDO)	Se enciende cuando la energía de CA está conectada a la unidad SVG1501. Indica que la energía está conectada correctamente.
RECEIVE (RECIBIR)	Destella mientras busca el canal receptor. Cambia a verde constante cuando se bloquea el canal de recepción.
SEND (ENVIAR)	Destella mientras busca el canal emisor. Cambia a verde constante cuando se bloquea el canal de envío.
ONLINE (EN LÍNEA)	Destella durante la registración y configuración de la unidad SVG1501. Cambia a verde constante cuando se registra la unidad SVG1501.

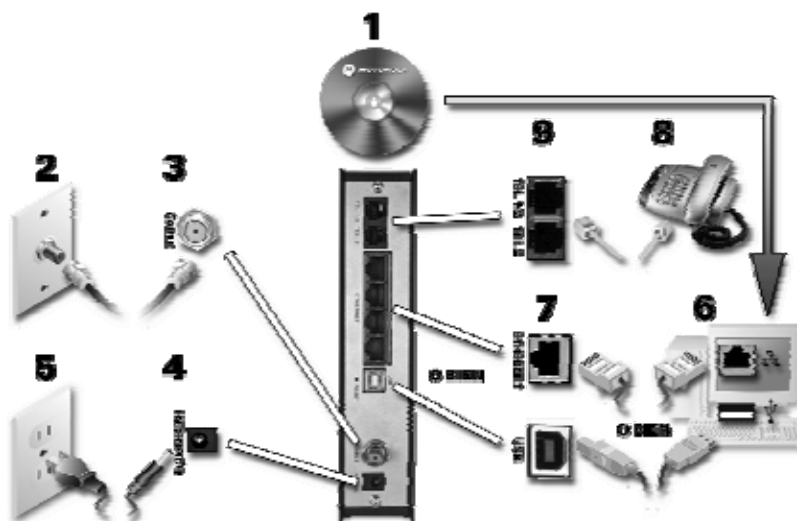
Conexión de la unidad SVG1501U

PRECAUCIÓN: Antes de enchufar el cable USB en SVG1501U, cargue el CD ROM de instalación de la unidad SVG1501 en la unidad de CD-ROM.

En ningún momento conecte los cables Ethernet y USB en el mismo equipo.

Antes de comenzar, asegúrese de que el equipo esté encendido y que el cable de alimentación de la unidad SVG1501U esté enchufado.

1. Inserte el CD-ROM de instalación de la unidad SVG1501 en la unidad de CD-ROM e instale los controladores USB que se apliquen.
2. Conecte uno de los extremos del cable coaxial al bifurcador o a la salida del cable.
3. Conecte el otro extremo del cable coaxial al conector de cable en la unidad SVG1501U. Ajuste manualmente los conectores para evitar dañarlos.
4. Enchufe el cable de alimentación en el puerto de encendido en la unidad SVG1501U.
5. Enchufe el otro extremo del cable de alimentación en un tomacorriente eléctrico.
Esto enciende automáticamente la puerta de enlace. No necesita desenchufar la puerta de enlace cuando no está en uso. La primera vez que enchufe la unidad SVG1501U, demorará de cinco a 30 minutos en encontrar y acoplarse a los canales de comunicación apropiados.
6. Conecte el cable USB o Ethernet al puerto apropiado en el equipo.
7. Conecte el otro extremo del cable USB o Ethernet al puerto apropiado en la puerta de enlace.



8. Conecte el cable telefónico de un teléfono de una o dos líneas al teléfono.

9. Conecte el otro extremo del cable telefónico de un teléfono de una o dos líneas al puerto TEL 1/2 en la parte posterior de la puerta de enlace.

Nota: Comuníquese con un proveedor de servicios de VoIP para activar este servicio.

10. Para un segundo teléfono, conecte el cable telefónico de un teléfono de una línea al puerto TEL 2 en la parte posterior de la unidad SVG1501.
11. Verifique que los indicadores LED en el panel frontal atraviesen la secuencia correcta. Consulte [Actividad del LED de la unidad SVG1501 durante el arranque](#).

Instalación en pared de la unidad SVG1501

Como opción, puede instalar la unidad SVG1501 en una pared:

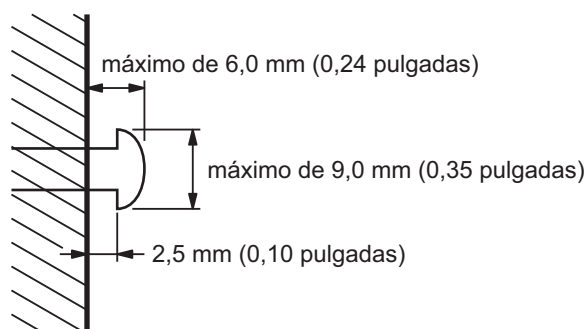
- Ubique la unidad según especifican los códigos locales o nacionales que rigen los servicios de comunicación y TV por cable residenciales o comerciales.
- Siga todos los estándares locales para la instalación de una unidad de interfaz de red (NIU) o dispositivo de interfaz de red (NID).
- Asegúrese de desconectar el enchufe de energía CA del tomacorriente y de retirar todos los cables de la parte posterior de la unidad SVG1501 antes de comenzar la instalación.
- Decida si desea instalar la unidad SVG1501 de manera horizontal o vertical.

Si es posible, instale la unidad en el hormigón, la mampostería, un travesaño de madera u otro material de pared sólido. Use soportes si fuese necesario (por ejemplo, si debe instalar la unidad en placas de yeso).

PRECAUCIÓN: Antes de taladrar, verifique la estructura para evitar daños potenciales en las líneas eléctricas, de agua o gas.

Haga lo siguiente para instalar su unidad SVG1501 en la pared:

1. Imprima una copia de la [Plantilla para la instalación en pared](#).
2. Mida la plantilla impresa con una regla para garantizar que tenga el tamaño correcto.
3. Use un punzón para marcar el centro de los orificios.
4. En la pared, ubique las marcas para los orificios de instalación.
5. Taladre a una profundidad de por lo menos 1 1/2 pulgadas (3,8 cm). Use tornillos M3,5 x 38 mm (#6 x 1 1/2 pulgadas) con cara interior plana y un diámetro máximo de cabeza de tornillo de 9,0 mm para instalar la unidad SVG1501.
6. Usando un destornillado, atornille cada tornillo hasta que parte del mismo sobresalga de la pared, como se muestra en la siguiente ilustración de las dimensiones de tornillos para la instalación en pared.



Debe haber 0,10 pulgadas (2,5 mm) entre la pared y la cara interior de la cabeza del tornillo.

7. Coloque la unidad SVG1501 para que los ojos de cerradura de la parte posterior de la unidad se alineen sobre los tornillos de instalación.
8. Deslice la unidad SVG1501 hacia abajo hasta que se trabe con la parte superior de la apertura del ojo de cerradura.
9. Luego de la instalación, vuelva a conectar la entrada de cable coaxial y la conexión de Ethernet.
10. Enchufe el cable de alimentación al conector +12 voltios de corriente continua (VCC) en la puerta de enlace de voz y el tomacorriente.
11. Coloque los cables en canales para evitar cualquier riesgo de seguridad.

Plantilla para la instalación en pared

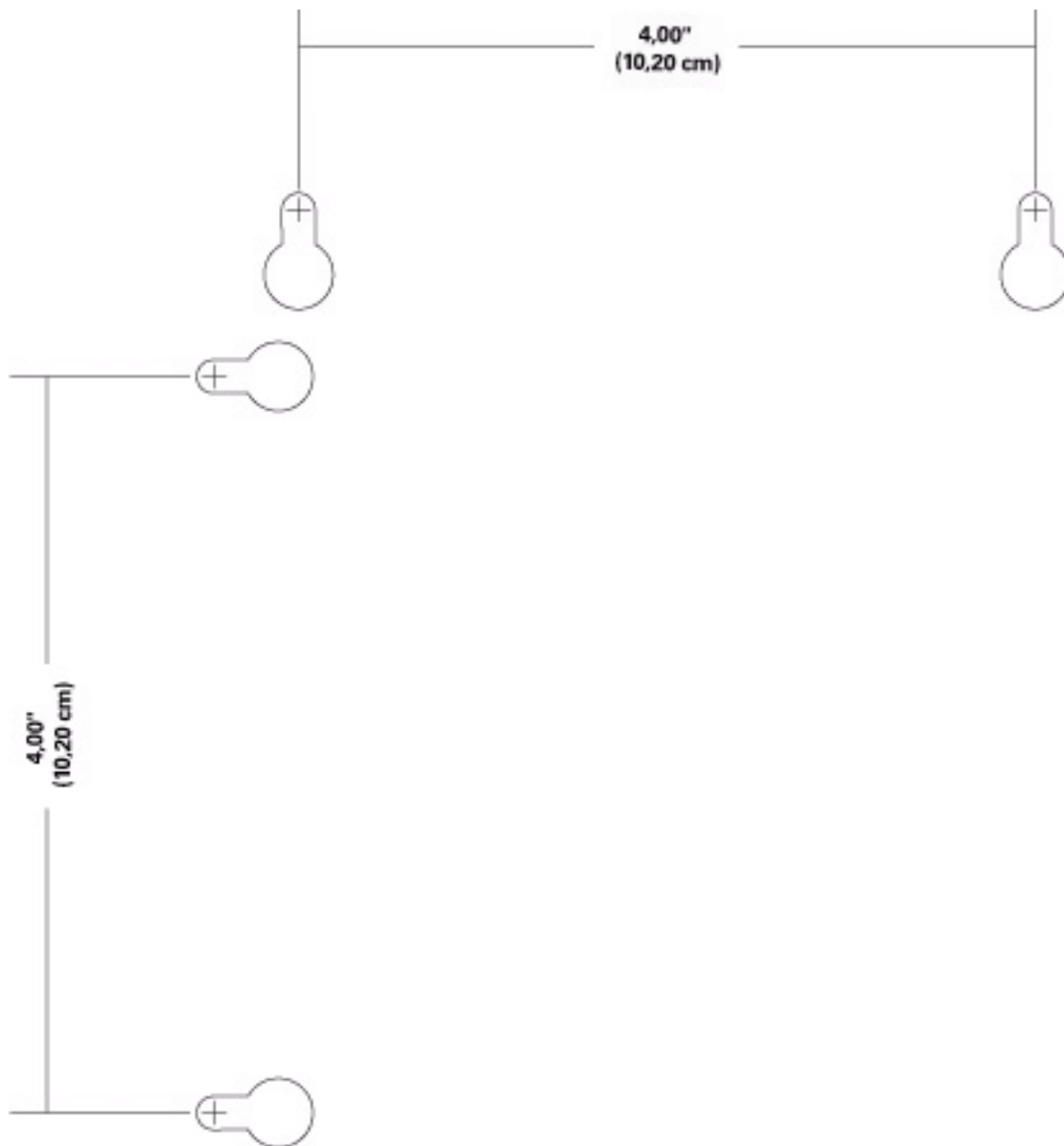


Figura 1 Plantilla para instalación en pared

Configuración del acceso a Internet

Luego de instalar la unidad SVG1501, verifique que pueda conectarse a Internet. Puede recuperar una dirección IP para la interfaz de red de su equipo usando una de las siguientes opciones:

- Recuperar la dirección IP y la dirección DNS definidas en forma estática
- Recuperar automáticamente la dirección IP usando el servidor DHCP de red

La puerta de enlace de voz inalámbrica Motorola SVG1501 proporciona un servidor DHCP en su red LAN. Motorola recomienda que configure su red LAN para obtener automáticamente las direcciones IP para la red LAN y el servidor DNS.

Asegúrese de que todos los equipos en su red LAN estén configurados para TCP/IP. Luego de configurar TCP/IP en su equipo, debe verificar la dirección IP.

Nota: Para sistemas UNIX o Linux, siga las instrucciones en la documentación del usuario aplicable.

Configuración de TCP/IP en Windows XP

1. Abra el **Panel de control**.
2. Haga doble clic en **Conexiones de red** para que se listen las conexiones de Internet de acceso telefónico y de red de área local (LAN) o de alta velocidad.
3. Haga clic con el botón secundario para conectarse con su interfaz de red.
4. Seleccione **Propiedades** del menú desplegable para que se muestre la ventana Propiedades de conexión de área local. Asegúrese que el Protocolo de Internet (TCP/IP) esté marcado.
5. Seleccione **Protocolo de Internet (TCP/IP)** y haga clic en **Propiedades** para mostrar la ventana Propiedades de protocolo Internet (TCP/IP).
6. Seleccione **Obtener una dirección IP automáticamente** y **Obtener la dirección del servidor DNS automáticamente**.
7. Haga clic en **Aceptar** para guardar la configuración de TCP/IP y salir de la ventana Propiedades de TCP/IP.
8. Cierre la ventana Propiedades de conexión de área local y salga del Panel de control.
9. Cuando finalice la configuración de TCP/IP, continúe con la Verificación de [la dirección IP en Windows XP](#).

Configuración de TCP/IP en Windows Vista

1. Abra el **Panel de control**.
2. Haga clic en **Red e Internet** para mostrar la ventana Red e Internet.
3. Haga clic en **Centro de redes y recursos compartidos** para mostrar la ventana Centro de redes y recursos compartidos.

4. Haga clic en **Administrar conexiones de red** para mostrar la ventana de conexiones a Internet de alta velocidad y de red de área local (LAN).
5. Haga clic con el botón secundario para elegir la interfaz de red que desea cambiar.
6. Haga clic en **Propiedades** para mostrar la ventana Propiedades de conexión de área local.
Vista puede solicitarle una confirmación o contraseña de administrador. Escriba la confirmación o la contraseña y luego haga clic en **Continuar**.
7. Haga clic en la pestaña **Funciones de red** y luego seleccione **Protocolo de Internet Versión 4 (IPv4)**.
8. Haga clic en **Propiedades** para mostrar la ventana Propiedades del Protocolo de Internet Versión 4 (TCP/IPv4).
9. Seleccione **Obtener una dirección IP automáticamente** y **Obtener la dirección del servidor DNS automáticamente**.
10. Haga clic en **Aceptar** para guardar la configuración de TCP/IP y cerrar la ventana Propiedades del Protocolo de Internet Versión 4 (TCP/IPv4).
11. Haga clic en **Aceptar** para cerrar la ventana Propiedades de conexión de área local.
12. Cierre las ventanas restantes y salga del Panel de control.
13. Cuando finalice la configuración de TCP/IP, continúe con la Verificación de la dirección IP en Windows Vista.

Verificación de la dirección IP en Windows XP

Para verificar la dirección IP:

1. En el escritorio de Windows, haga clic en **Inicio**.
2. Seleccione **Ejecutar**. Aparecerá la ventana Ejecutar.
3. Escriba **cmd** y haga clic en **Aceptar**.
4. Escriba **ipconfig** y presione **INTRO** para mostrar su configuración de IP.

Si aparece una dirección IP de configuración automática, esto indica posibles problemas de red de cable o una conexión incorrecta entre su equipo y la unidad SVG1501.

Verifique lo siguiente:

- Sus conexiones de cable
- Si puede ver los canales de TV por cable en su televisor

Luego de verificar con éxito sus conexiones de cable y el funcionamiento correcto de su TV por cable, puede renovar su dirección IP.

Verificación de la dirección IP en Windows Vista

Haga lo siguiente para verificar la dirección IP:

1. En el escritorio de Windows, haga clic en **Inicio**.
2. Haga clic en **Todos los programas**.
3. Haga clic en **Accesorios**.

4. Haga clic en **Símbolo del sistema** para abrir una ventana de símbolo del sistema.
5. Escriba **ipconfig** y presione **INTRO** para mostrar su dirección IP.

Si aparece una dirección IP de configuración automática, esto indica una conexión incorrecta entre su equipo y la unidad SVG1501, u otros posibles problemas de red de cable.

Renovación de su dirección IP

Para renovar su dirección IP en Windows XP o Windows Vista:

1. Abra la ventana de símbolo del sistema.
2. Escriba **ipconfig / renew** en el símbolo del sistema y presione **INTRO** para obtener una nueva dirección IP.
3. Escriba **exit** y presione **INTRO** para cerrar la ventana del símbolo del sistema.

Si luego de realizar este procedimiento su computadora no puede obtener acceso a Internet, comuníquese con su proveedor de servicio de cable para obtener ayuda.

Configuración de una red Wi-Fi

Haga lo siguiente para configurar una red Wi-Fi usando el botón WPS en la unidad SVG1501:

1. Encienda la puerta de enlace de voz inalámbrica SVG1501.
2. Encienda los dispositivos habilitados para WPS que desea que tengan acceso a la red, como una PC, un enrutador o un teléfono.

La red Wi-Fi detectará automáticamente los dispositivos WPS.

3. Presione el botón **WPS** en la unidad SVG1501.
4. Si se aplica, presione el botón **WPS** en los otros dispositivos WPS.

3

Configuración básica

Para el funcionamiento normal, no necesita cambiar las configuraciones predeterminadas.

PRECAUCIÓN: Para evitar configuraciones no autorizadas, cambie la contraseña predeterminada inmediatamente cuando configure por primera vez la unidad SVG1501. Consulte [Cambio de la contraseña predeterminada de la unidad SVG1501](#).

Los firewalls no son infalibles. Elija la política de firewall más segura que pueda. Consulte [Páginas de firewall](#) para obtener más información.

Inicio del administrador de configuración (CMGR) de la unidad SVG1501

Use el administrador de configuración (CMGR) de la unidad SVG1501 para cambiar y ver las configuraciones de su unidad SVG1501.

1. Abra el explorador Web en un equipo conectado a la unidad SVG1501 a través de una conexión de Ethernet.

Nota: No intente configurar la unidad SVG1501 a través de una conexión inalámbrica.

2. En el campo "Address" (Dirección) o "Location" (Ubicación) de su explorador, escriba **http://192.168.0.1** y presione **INTRO**.
3. Escriba **admin** en el campo "Username" (Nombre de usuario). Este campo distingue entre mayúsculas y minúsculas.
4. Escriba **motorola** en el campo "Password" (Contraseña). Este campo distingue entre mayúsculas y minúsculas.

Login

Login
Please enter username and password to login.

Username

Password

5. Haga clic en **Login (Inicio de sesión)** para mostrar la página de estado de conexión de la unidad SVG1501.

Startup Procedure			
Procedure	Status	Comment	
Acquire Downstream Channel		Locked	
Connectivity State	OK	Operational	
Boot State	OK	Operational	
Configuration File			
Security	Disabled	Disabled	
Downstream Channel			
Lock Status	Locked	Modulation	QAM64
Channel ID	0	Symbol rate	5056941
Downstream Frequency	447000000 Hz	Downstream Power	14.3 dBmV
SNR	36.4 dBmV		
Upstream Channel			
Lock Status	Locked	Modulation	QAM16
Channel ID	1	Symbol rate	640 Ksym/sec
Upstream Frequency	21008000 Hz	Upstream Power	28.5 dBmV
CM IP Address	Duration	Expires	
-----	D -- H -- M -- S --	-----	

La página "Status Connection" (Estado de conexión) brinda información de estado de los canales receptores y emisores de radiofrecuencia en la conexión de red de la unidad SVG1501.

Si tiene problemas para iniciar el administrador de configuración (CMGR) de la unidad SVG1501, consulte [Solución de problemas](#) para obtener más información.

Barra del menú Opciones de la unidad SVG1501

La barra del menú Opciones de la unidad SVG1501 aparece en la parte superior de la ventana del administrador de configuración de la unidad SVG1501.



Barra del menú Opciones del administrador de configuración

Páginas del menú Opciones	Función
Status (Estado)	Brinda información sobre el hardware y el software de la unidad SVG1501, la dirección MAC, la dirección IP de la puerta de enlace de voz, el número de serie e información relacionada. Otras páginas brindan herramientas de diagnóstico y le permiten cambiar el nombre de usuario y contraseña de su unidad SVG1501.
Basic (Opciones básicas)	Muestra y configura los ajustes relacionados con en IP de la unidad SVG1501, incluida la configuración de red, el tipo de conexión de red WAN,

Páginas del menú Opciones	Función
	el protocolo de control dinámico de host (DHCP) y el sistema de nombre de dominio dinámico (DDNS).
Advanced (Opciones avanzadas)	Configura y supervisa el enrutamiento del tráfico IP que efectúa la unidad SVG1501
Firewall (Firewall)	Configura y supervisa el firewall de la unidad SVG1501
Parental Control (Control para padres)	Configura y supervisa la función de control para padres de la unidad SVG1501
Wireless (Redes inalámbricas)	Configura y supervisa la función de redes inalámbricas de la unidad SVG1501
VPN (Red privada virtual)	Configura y supervisa el funcionamiento de la unidad SVG1501 con una red privada virtual (VPN)
MTA (Adaptador terminal multimedia)	Supervisa las funciones telefónicas de la unidad SVG1501
Logout (Salir)	Salte del administrador de configuración de la unidad SVG1501

Obtención de ayuda

Para recuperar la información de ayuda para cualquier opción del menú, haga clic en **help (ayuda)** en esa página.

Cómo salir del administrador de configuración de la unidad SVG1501

Para cerrar sesión y cerrar el administrador de configuración de SVG1501:

- Haga clic en **Logout (Salir)** en la barra del menú Opciones de la unidad SVG1501.

4

Páginas de estado

Use las páginas de Estado de la unidad SVG1501 para obtener información sobre el hardware y el software de la unidad SVG1501, la dirección MAC, la dirección IP del cable módem y el número de serie; para supervisar su conexión del sistema de cable; para obtener acceso a las herramientas de diagnóstico adicionales; y para cambiar el nombre de usuario y contraseña de su unidad SVG1501.

Página de estado del software

Muestra la información sobre la versión de hardware, la versión de software, la dirección MAC, la dirección IP del cable módem, el número de serie, el tiempo de funcionamiento del sistema y el estado del registro de la red.

Information	
Standard Specification Compliant	DOCSIS 2.0
Hardware Version	1
Software Version	SVG1501E-2.9.9.9-LAB-98-98-SH
Cable Modem MAC Address	00:1e:5a:8c:e1:1a
Cable Modem Serial Number	150100000000000000000003
CM certificate	Installed
Status	
System Up Time	25 days 04h:59m:58s
Network Access	Denied
Cable Modem IP Address	www.pppwww.pppwww

Página de estado de la conexión

Verifique el estado de conectividad de la red IP y HFC de la unidad SVG1501.

- Haga clic en el botón **Refresh (Actualizar)** en su explorador Web para actualizar la información.

Startup Procedure			
Procedure	Status	Comment	
Acquire Downstream Channel		Locked	
Connectivity State	OK	Operational	
Boot State	OK	Operational	
Configuration File			
Security	Disabled	Disabled	
Downstream Channel			
Lock Status	Locked	Modulation	QAM64
Channel ID	0	Symbol rate	5056941
Downstream Frequency	447000000 Hz	Downstream Power	13.1 dBmV
SNR	37.7 dBmV		
Upstream Channel			
Lock Status	Locked	Modulation	QAM16
Channel ID	1	Symbol rate	640 Ksym/sec
Upstream Frequency	21008000 Hz	Upstream Power	31.0 dBmV
CM IP Address	Duration	Expires	
-----	D: -- H: -- M: -- S: --	-----	

Página de estado de la seguridad

Defina los privilegios de acceso del administrador cambiando el nombre de usuario y la contraseña de su unidad SVG1501, y restablezca su nombre de usuario y contraseña a la configuración predeterminada.

Change User Information	
Password Change Username	<input type="text"/>
New Password	<input type="text"/>
Re-Enter New Password	<input type="text"/>
Current Username Password	<input type="text"/>
Restore Factory Defaults	
<input type="radio"/> Yes	<input checked="" type="radio"/> No
<input type="button" value="Apply"/>	

Cambio de la contraseña predeterminada de la unidad SVG1501

PRECAUCIÓN: Para evitar configuraciones no autorizadas, cambie la contraseña predeterminada inmediatamente cuando configure por primera vez su unidad Motorola SVG1501.

1. Escriba su nuevo nombre de usuario en el campo "Password Change Username" (Nombre de usuario de cambio de contraseña).
2. Escriba su nueva contraseña en el campo "New Password" (Nueva contraseña). Este campo distingue entre mayúsculas y minúsculas.

3. Escriba nuevamente su nueva contraseña en el campo "Re-Enter New Password" (Vuelva a ingresar nueva contraseña). Este campo distingue entre mayúsculas y minúsculas.
4. Escriba su contraseña anterior en el campo "Current Username Password" (Contraseña de nombre de usuario actual).
5. Seleccione **Yes (Sí)** si desea restablecer el nombre de usuario y la contraseña a la configuración original de fábrica.
6. Haga clic en **Apply (Aplicar)** para actualizar la contraseña del nombre de usuario.

***Nota:** Debe iniciar sesión con el nombre de usuario predeterminado (**admin**) y la contraseña predeterminada (**motorola**) luego de aplicar el cambio de restaurar las configuraciones de fábrica.*

Restauración los valores predeterminados de fábrica

Para restablecer el nombre de usuario y la contraseña a la configuración original de fábrica:

1. Seleccione **Yes (Sí)** y haga clic en **Apply (Aplicar)**.
2. Inicie sesión con el nombre de usuario predeterminado (**admin**) y la contraseña predeterminada (**Motorola**) luego de aplicar este cambio. Todas las entradas distinguen entre mayúsculas y minúsculas.

Página de estado del diagnóstico

Utilice las siguientes herramientas de diagnóstico para resolver problemas de conectividad IP:

- Ping (LAN)
- Encaminamiento de rastreo (WAN)

Herramienta Ping

Use la herramienta Ping (agrupador de paquetes de Internet) para verificar la conectividad entre la unidad SVG1501 y otros dispositivos en la red LAN de la unidad SVG1501 enviando un pequeño paquete de datos y luego esperando una respuesta. Una respuesta Ping confirma que el equipo está conectado a la unidad SVG1501.

Select Utility	
Ping	
Ping Test Parameters	
Target	192 .168 .0 .1
Ping Size	64 bytes
No. of Pings	3
Ping Interval	1000 ms
Start Test	Abort Test
Clear Results	
Results	
Pinging 192.168.0.1 with 64 bytes of data:[Complete] Reply from 192.168.0.1: bytes = 64, time = 0 ms Reply from 192.168.0.1: bytes = 64, time = 0 ms Reply from 192.168.0.1: bytes = 64, time = 0 ms 3/3 replies received. min time=0 ms, max time=10 ms, avg time=0 ms	

Prueba de conectividad de red con la unidad SVG1501

Para verificar la conectividad entre la unidad SVG1501 y otros dispositivos en la red LAN de la unidad SVG1501, realice la siguiente prueba:

1. Seleccione **Ping (Ping)** de la lista desplegable "Select Utility" (Seleccionar herramienta).
2. En el campo "Target" (Destino) ingrese la dirección IP del equipo en que desea realizar la comprobación Ping.
3. En el campo "Ping Size" (Tamaño de Ping) ingrese el tamaño de paquete de datos en bytes.
4. En el campo "No. of Pings" (Nº de pings) ingrese el número de intentos de ping.
5. En el campo "Ping Interval" (Intervalo de pings) ingrese el tiempo entre las operaciones de envío de Ping en milisegundos.
6. Haga clic en **Start Test (Iniciar prueba)** para iniciar la operación Ping. Los resultados de la operación Ping se mostrarán en el panel "Results" (Resultados).
7. Puede hacer clic en **Abort Test (Abandonar prueba)** en cualquier momento durante la prueba para detener la operación Ping.
8. Repita del paso 2 al 6 para cada dispositivo en el que desee realizar la comprobación Ping.

Cunado haya finalizado, haga clic en **Clear Results (Borrar resultados)** para eliminar los resultados de Ping en el panel "Results" (Resultados).

Herramienta Encaminamiento de rastreo

Use la herramienta de encaminamiento de rastreo para asignar la ruta de red desde el administrador de configuración de la unidad SVG1501 hasta el host público.

Select Utility	
Traceroute	

Traceroute Parameters	
Target	IP address or Name
Max Hops	255
Data Size	32 bytes
Base Port	33434
Resolve Host	Off

Start Test Clear Results

Results
Waiting for input...

1. En el campo "Target" (Destino) ingrese la dirección IP o nombre de host del equipo en que desea realizar el encaminamiento de rastreo.
2. En el campo "Max Hops" (Máximo de saltos) ingrese el número máximo de saltos que la operación de encaminamiento de rastreo realiza antes de detenerse.
3. En el campo "Data Size" (Tamaño de datos) ingrese el tamaño de paquete de datos en bytes.
4. En el campo "Base Port" (Puerto base) establezca el número de puerto UDP base utilizado por la operación de encaminamiento de rastreo. El predeterminado es **33434**. Si un puerto UDP no está disponible, este campo se puede utilizar para especificar un rango de puertos no utilizados.
5. En el campo "Resolve Host" (Resolver host) seleccione **On (Activado)** para listar los nombres de hosts encontrados durante la operación de encaminamiento de rastreo, o seleccione **Off (Desactivado)** para listar únicamente las direcciones IP de hosts.
6. Luego de ingresar los parámetros de encaminamiento de rastreo, haga clic en **Start Test (Iniciar prueba)** para iniciar la operación de encaminamiento de rastreo. Los resultados de la operación de encaminamiento de rastreo se mostrarán en el panel "Results" (Resultados).
7. Cuando haya finalizado, haga clic en **Clear Results (Borrar resultados)** para eliminar los resultados de encaminamiento de rastreo en el panel "Results" (Resultados).

Página de estado del registro de eventos

Revise los eventos críticos del sistema en orden cronológico en el registro de eventos del protocolo de administración de red simple (SNMP).

Time	Priority	Description
Time Not Established	Critical (3)	SYNC Timing Synchronization failure - Failed to acquire QAM/Q...
Time Not Established	Notice (6)	Ds Lock Failed - Reinitialize MAC...
Time Not Established	Critical (3)	SYNC Timing Synchronization failure - Failed to acquire QAM/Q...
Time Not Established	Notice (6)	Ds Lock Failed - Reinitialize MAC...
Time Not Established	Critical (3)	SYNC Timing Synchronization failure - Failed to acquire QAM/Q...
Time Not Established	Notice (6)	Ds Lock Failed - Reinitialize MAC...
Time Not Established	Critical (3)	SYNC Timing Synchronization failure - Failed to acquire QAM/Q...
Time Not Established	Critical (3)	SYNC Timing Synchronization failure - Failed to acquire FEC f...
Time Not Established	Critical (3)	SYNC Timing Synchronization failure - Failed to acquire QAM/Q...
Time Not Established	Notice (6)	Ethernet link up - ready to pass packets
Thu Nov 13 14:47:40 2008	Notice (6)	Modem Is Shutting Down and Rebooting...
Thu Nov 13 14:47:40 2008	Critical (3)	Received Response to Broadcast Maintenance Request, But no Un...
Thu Nov 13 14:47:40 2008	Critical (3)	SYNC Timing Synchronization failure - Failed to acquire QAM/Q...
Thu Nov 13 14:43:54 2008	Information (7)	Registration Completed
Thu Nov 13 14:43:54 2008	Information (7)	Authorized
Thu Nov 13 14:43:54 2008	Information (7)	Retrieved Time..... SUCCESS
Thu Nov 13 14:43:54 2008	Information (7)	Retrieved TFTP Config sbv5200_cm_dual_1.1_dqos_full_pc_sbvpro...
Thu Nov 13 14:43:54 2008	Information (7)	Retrieved DHCP SUCCESS
Thu Nov 13 14:43:47 2008	Information (7)	Acquired Upstream SUCCESS
Thu Nov 13 14:43:43 2008	Information (7)	Acquired Downstream (651038118 Hz)..... SUCCESS
Thu Nov 13 14:43:32 2008	Notice (6)	Ds Lock Failed - Reinitialize MAC...
Thu Nov 13 14:43:32 2008	Information (7)	Retrieved Time..... SUCCESS
Thu Nov 13 14:43:32 2008	Information (7)	Retrieved TFTP Config sbv5200_cm_dual_1.1_dqos_full_pc_sbvpro...
Time Not Established	Information (7)	Retrieved DHCP SUCCESS
Time Not Established	Information (7)	Acquired Upstream SUCCESS

5

Páginas básicas

Vea y configure los ajustes relacionados con en IP de la unidad SVG1501, incluida la configuración de red, el tipo de conexión de red WAN, el protocolo de control dinámico de host (DHCP) y el sistema de nombre de dominio dinámico (DDNS) en las páginas básicas. La opción de copia de seguridad le permite guardar una copia de la configuración de su unidad SVG1501 en su equipo

Página básica de configuración

Configure las funciones básicas de su puerta de enlace SVG1501 relacionadas con la conexión de su proveedor de servicios de Internet (ISP).

Primary Mode	
NAPT mode	Enabled
Changes may require a reboot to take effect.	
Apply	
Network Configuration	
LAN IP Address	192 . 168 . 0 . 1
MAC Address	00:21:80:d2:80:15
WAN IP Address	---
MAC Address	00:21:80:d2:80:16
Duration	D: -- H: -- M: -- S: --
Expires	---
<input type="button" value="Release WAN Lease"/> <input type="button" value="Renew WAN Lease"/>	
WAN Connection Type	
DHCP	
Host Name	(Required by some ISPs)
Domain Name	(Required by some ISPs)
MTU Size	0 (256-1500 octets, 0 = use default)
Spoofed MAC Address	00 : 00 : 00 : 00 : 00 : 00
Changes may require a reboot to take effect.	
Apply	

Descripciones de campos para la página básica de configuración

Campo	Descripción
NAPT mode (Modo NAPT)	<p>La traducción del puerto de dirección de red (NAPT) es un caso especial de la traducción de dirección de red (NAT) donde varios números IP se ocultan detrás de un número de direcciones. Sin embargo, en contraposición a la traducción NAT original, ésta no implica que puedan existir únicamente ese número de conexiones en un determinado momento.</p> <p>En el modo NAPT se realiza una multiplexación de un número casi arbitrario de conexiones a través de la información de puerto TCP. Este número de conexiones simultáneas se ve limitado por el número de direcciones multiplicado por el número de puertos TCP disponibles.</p>

Campo	Descripción
LAN (Red de área local)	Ingrese la dirección IP de la unidad SVG1501 en su red LAN privada.
IP Address (Dirección IP)	Dirección de control de acceso de medios: conjunto de 12 dígitos hexadecimales asignados durante la fabricación que identifican distintivamente la dirección de hardware del punto de acceso de la unidad SVG1501.
MAC Address (Dirección MAC)	Dirección de control de acceso de medios: conjunto de 12 dígitos hexadecimales asignados durante la fabricación que identifican distintivamente la dirección de hardware del punto de acceso de la unidad SVG1501.
WAN (Red de área extensa)	Dirección IP de la red WAN pública de su dispositivo SVG1501, asignada de manera dinámica o estática por su proveedor de servicios de Internet (ISP).
IP Address (Dirección IP)	Dirección de control de acceso de medios: conjunto de 12 dígitos hexadecimales asignados durante la fabricación que identifican distintivamente la dirección de hardware del punto de acceso de la unidad SVG1501.
MAC Address (Dirección MAC)	Describe el tiempo que transcurrirá antes de que caduque su conexión de Internet. La concesión de la red WAN se renovará automáticamente cuando caduque.
Duration (Duración)	Muestra la hora y la fecha exactas cuando caduca la concesión de la red WAN.
Expires (Vencimiento)	Haga clic para liberar la concesión de la red WAN.
Release WAN Lease (Liberar concesión de la red WAN)	Haga clic para renovar la concesión de la red WAN.
Renew WAN Lease (Renovar concesión de la red WAN)	DHCP o IP estático. Si su proveedor de servicios de Internet (ISP) utiliza DHCP, seleccione DHCP (DHCP) e ingrese el nombre de host y el nombre de dominio, si se requiere. Si su proveedor de servicios de Internet (ISP) utiliza una dirección de IP estática, seleccione Static IP (IP estática) e ingrese la información suministrada por su ISP para la dirección de IP estática, máscara de IP estática, puerta de enlace predeterminada, DNS principal y DNS secundaria.
WAN Connection Type (Tipo de conexión de la red WAN)	Si su tipo de conexión de la red WAN es DHCP, ingrese un nombre de host, si se requiere.
Host Name (Nombre de host)	Si su tipo de conexión de la red WAN es DHCP, ingrese un nombre de dominio, si se requiere.
Domain Name (Nombre de dominio)	

Campo	Descripción
MTU Size (Tamaño de MTU)	La unidad máxima de transmisión (MTU) es el tamaño más grande de paquete o marco que se puede enviar. El valor predeterminado es apropiado para la mayoría de los usuarios.
Spoofed MAC Address (Dirección MAC suplantada)	Si su tipo de conexión de red WAN es IP estática, ingrese la información suministrada por su ISP para la dirección de IP estática, máscara de IP estática, puerta de enlace predeterminada, DNS principal y DNS secundaria.

Cuando haya finalizado, haga clic en **Apply (Aplicar)** para guardar sus cambios.

Página básica del protocolo DHCP

Configure y vea el estado del servidor opcional interno DHCP (protocolo de configuración de host dinámico) de la unidad SVG1501 para la red LAN.

DHCP

DHCP Server	<input checked="" type="radio"/> Yes <input type="radio"/> No
Starting Local Address	192.168.0.10
Number of CPEs	245
Lease Time	3600

DHCP Clients

MAC Address	IP Address	Subnet Mask	Duration	Expires	Select
000a5e510499	192.168.000.014	255.255.255.000	D:00 H:01 M:00 S:00	----- ----- ----- -----	<input checked="" type="radio"/>

WINS Addresses

<input type="text"/>	<input type="button" value="Add Primary"/>	<input type="button" value="Add Secondary"/>
<input type="button" value="Add Tertiary"/>		
Primary: 0.0.0.0		
Secondary: 0.0.0.0		
Tertiary: 0.0.0.0		
<input type="button" value="Remove WINS Address"/>		<input type="button" value="Clear All"/>

Current System Time:-----:--:--

PRECAUCIÓN: No modifique esta configuración a menos que sea un administrador de red con experiencia y conocimiento sólido en direcciones IP, subredes y DHCP.

Descripciones de campos para la página básica del protocolo DHCP

Campo	Descripción
DHCP Server (Servidor DHCP)	<p>Seleccione Yes (Sí) para habilitar el servidor DHCP de la unidad SVG1501.</p> <p>Seleccione No (No) para deshabilitar el servidor DHCP de la unidad SVG1501.</p>
Starting Local Address (Dirección local de inicio)	<p>Ingrese la dirección IP de inicio que asignará el servidor DHCP de la unidad SVG1501 a los clientes en el formato de decimales separados por puntos. El valor predeterminado es 192.168.0.2.</p>
Number of CPEs (Número de equipos terminales del cliente)	<p>Establece el número de clientes para que el servidor DHCP de la unidad SVG1501 asigne una dirección IP privada. Hay 245 direcciones de cliente posibles. El valor predeterminado es 245.</p>
Lease Time (Tiempo de concesión)	<p>Establece el tiempo en segundos en que el servidor DHCP de la unidad SVG1501 concede una dirección IP para un cliente. El valor predeterminado es 3600 segundos (60 minutos).</p>
DHCP Clients (Clientes DHCP)	<p>Lista la información del dispositivo cliente DHCP.</p>
WINS Addresses (Direcciones WINS)	<p>Especifica hasta tres direcciones de servidor del servicio de nombres de Internet de Windows (WINS).</p>

Haga clic en **Apply (Aplicar)** para guardar sus cambios.

Para renovar una dirección IP del cliente DHCP, haga clic en **Select (Seleccionar)** y luego en **Force Available (Forzar disponible)**.

Página básica de DDNS

Configura el servicio del sistema de nombre de dominio dinámico (DDNS) para asignar un nombre de dominio de Internet estático a una dirección IP dinámica. Esto permite que se pueda obtener acceso fácil a su unidad SVG1501 desde varias ubicaciones en Internet.

DDNS	
DDNS Service:	Disabled
User Name:	<input type="text"/>
Password:	<input type="password"/>
Host Name:	<input type="text"/>
IP Address:	0.0.0.0
Status:	DDNS service is not enabled.
<input type="button" value="Apply"/>	

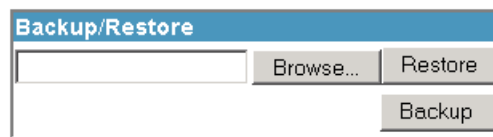
Descripciones de campos para la página básica de DDNS

Campo	Descripción
DDNS Service (Servicio DDNS)	Seleccione Disable (Deshabilitar) o wwwDynDNS.org para habilitar el servicio DDNS.
User Name (Nombre de usuario)	Ingrese el nombre de usuario de su DDNS.
Password (Contraseña)	Ingrese la contraseña de su DDNS.
Host Name (Nombre de host)	Ingrese el nombre de host de su DDNS.
IP Address (Dirección IP)	Detalla la información de IP.
Status (Estado)	Muestra el estado de servicio de DDNS: enabled (habilitado) o disabled (deshabilitado)

Haga clic en **Apply (Aplicar)** para guardar sus cambios.

Página básica de copia de seguridad

Guarde los ajustes de configuración actuales de su unidad SVG1501 de manera local en su equipo o restaure las configuraciones guardadas previamente.



The screenshot shows a window titled "Backup/Restore". It contains a text input field for a file path, a "Browse..." button to the right of the field, a "Restore" button to the right of the "Browse..." button, and a "Backup" button centered below the "Restore" button.

Restauración de la configuración de su unidad SVG1501

1. Escriba la ruta con el nombre de archivo donde está ubicado el archivo de copia de seguridad en su equipo o haga clic en **Browse (Examinar)** para ubicar el archivo.
2. Haga clic en **Restore (Restaurar)** para recrear los ajustes de su unidad SVG1501 previamente guardados.

Copia de seguridad de la configuración de su unidad SVG1501

1. Escriba la ruta con el nombre de archivo donde desea almacenar el archivo de copia de seguridad en su equipo o haga clic en **Browse (Examinar)** para ubicar el archivo.
2. Haga clic en **Backup (Copia de seguridad)** para crear una copia de seguridad de los ajustes de su unidad SVG1501.

6

Páginas avanzadas

Configura los ajuste de filtrado de IP, filtrado de MAC, filtrado de puertos, reenvío de puertos, disparadores de puertos, host de DMZ y protocolo de información de enrutamiento (RIP).

Haga clic en cualquier opción del submenú avanzado para ver o cambiar la información de configuración avanzada para dicha opción.

Página avanzada de opciones

Establece los modos operativos para ajustar la manera en que el dispositivo SVG1501 enruta el tráfico IP.

Descripciones de campos para la página avanzada de opciones

Campo	Descripción
WAN Blocking (Bloqueo de WAN)	Evita que el administrador de configuración de la unidad SVG1501 o las PC detrás de éste puedan ser vistos por otros equipos en la red WAN de la unidad SVG1501. Seleccione Enable (Habilitar) para activar esta opción.
IPsec PassThrough (Transferencia de IPsec)	Permite que el protocolo de transferencia de IPsec se pueda utilizar a través del administrador de configuración de la unidad SVG1501 para que un dispositivo de VPN (o software) se pueda comunicar correctamente con la red WAN.

Campo	Descripción
	Seleccione Enable (Habilitar) para activar esta opción.
PPTP PassThrough (Transferencia de PPTP)	Permite que el protocolo de transferencia para túnel de punto a punto (PPTP) se pueda utilizar a través del administrador de configuración de la unidad SVG1501 para que un dispositivo de VPN (o software) se pueda comunicar correctamente con la red WAN. Seleccione Enable (Habilitar) para activar esta opción.
Remote Config Management (Administración de configuración remota)	Permite el acceso remoto al administrador de configuración de la unidad SVG1501. Esto permite que configure la red WAN de la unidad SVG1501 al obtener acceso a la dirección IP de la red WAN en el puerto 8080 del administrador de configuración desde cualquier lugar en Internet. Por ejemplo, escriba http://WanIPAddress:8080/ en la ventana de la URL del explorador para obtener acceso remoto al administrador de configuración de la unidad SVG1501. Seleccione Enable (Habilitar) para activar esta opción.
Multicast Enable (Habilitar multidifusión)	Permite que el tráfico específico de multidifusión (indicada por una dirección específica de multidifusión) se transmita a y desde las PC en la red privada detrás del administrador de configuración. Seleccione Enable (Habilitar) para activar esta opción.
UPnP Enable (Habilitar UPnP)	Activa el agente del protocolo universal de conexión y funcionamiento (UPnP) en el administrador de configuración. Si está ejecutando una aplicación CPE (cliente) que requiere UPnP, seleccione esta casilla. Seleccione Enable (Habilitar) para activar esta opción.
Rg PassThrough (Transferencia de Rg)	Deshabilita la operación NAT y permite que todos los equipos cliente actúen como clientes de transferencia. Seleccione Enable (Habilitar) para activar esta opción.
PassThrough Mac Addresses (Direcciones MAC de transferencia)	Especifica hasta 32 equipos como clientes de transferencia no sujetos a NAT, a través de sus direcciones MAC. Para habilitar esta función, es posible que su operador de cable deba suministrarle direcciones IP públicas adicionales.

Haga clic en **Apply (Aplicar)** para guardar los cambios.

Página avanzada de filtrado de IP

Define los equipos locales a los que se les negará el acceso a la red WAN de la unidad SVG1501 al configurar los filtros de direcciones IP para bloquear el tráfico de Internet a dispositivos de red específicos en la red LAN. Ingrese el valor LSB (byte menos significativo) de la dirección IP; los bytes superiores de la dirección IP se establecen automáticamente de la dirección IP del administrador de configuración de la unidad SVG1501.

Puede almacenar la configuración de filtros comúnmente utilizada pero no tenerla activa.

IP Filtering		
Start Address	End Address	Enabled
192.168.0. <input type="text" value="0"/>	192.168.0. <input type="text" value="0"/>	<input type="checkbox"/>
192.168.0. <input type="text" value="0"/>	192.168.0. <input type="text" value="0"/>	<input type="checkbox"/>
192.168.0. <input type="text" value="0"/>	192.168.0. <input type="text" value="0"/>	<input type="checkbox"/>
192.168.0. <input type="text" value="0"/>	192.168.0. <input type="text" value="0"/>	<input type="checkbox"/>
192.168.0. <input type="text" value="0"/>	192.168.0. <input type="text" value="0"/>	<input type="checkbox"/>
192.168.0. <input type="text" value="0"/>	192.168.0. <input type="text" value="0"/>	<input type="checkbox"/>
192.168.0. <input type="text" value="0"/>	192.168.0. <input type="text" value="0"/>	<input type="checkbox"/>
192.168.0. <input type="text" value="0"/>	192.168.0. <input type="text" value="0"/>	<input type="checkbox"/>
192.168.0. <input type="text" value="0"/>	192.168.0. <input type="text" value="0"/>	<input type="checkbox"/>
192.168.0. <input type="text" value="0"/>	192.168.0. <input type="text" value="0"/>	<input type="checkbox"/>
<input type="button" value="Apply"/>		

Descripciones de campos para la página avanzada de filtrado de IP

Campo	Descripción
Start Address (Dirección de inicio)	Ingrese el rango de dirección IP de inicio de los equipos a los que les desee denegar acceso a la red WAN de la unidad SVG1501. Ingrese únicamente el byte menos significativo de la dirección IP.
End Address (Dirección de finalización)	Ingrese el rango de dirección IP de finalización de los equipos a los que les desee denegar acceso a la red WAN de la unidad SVG1501. Ingrese únicamente el byte menos significativo de la dirección IP.
Enabled (Habilitado)	Active el filtro de dirección IP. Seleccione cada rango de direcciones IP a las que les desee denegar el acceso a la red WAN de la unidad SVG1501.

Haga clic en **Apply (Aplicar)** para activar y guardar su configuración.

Página avanzada de filtrado de MAC

Defina hasta 20 filtros de direcciones de control de acceso de medios (MAC) para evitar que las PC envíen tráfico TCP/UDP saliente a la red WAN a través de sus direcciones MAC. La dirección MAC de una tarjeta NIC específica nunca cambia, a diferencia de su dirección IP que se puede asignar a través del servidor DHCP o se puede definir de modo predeterminado en varias direcciones con el tiempo.

Descripciones de campos para la página avanzada de filtrado de MAC

Campo	Descripción
MAC Address (Direcciones MAC)	Dirección de control de acceso de medios: conjunto de 12 dígitos hexadecimales asignados a una PC durante la fabricación.

Configuración de un filtro de dirección MAC

1. Ingrese la dirección MAC en el campo "MAC Addresses" (Direcciones MAC) para la PC que desea bloquear.
2. Haga clic en **Add MAC Address (Agregar dirección MAC)**.
3. Repita los pasos anteriores para hasta veinte direcciones MAC.

Página avanzada de filtrado de puerto

Defina los filtros de puertos para evitar que ningún dispositivo envíe tráfico TCP/UDP saliente a la red WAN en números de puertos IP específicos. Especifique un rango de puerto de inicio y finalización para determinar el tráfico TCP/UDP saliente a la red WAN que se permite por puerto.

Nota: Los rangos de puertos específicos se bloquean para TODAS las PC. Esta configuración no es específica de la dirección IP o dirección MAC. Por ejemplo, para bloquear todas las PC en la red LAN privada para que no obtengan acceso a sitios HTTP, establezca el "Start Port" (Puerto de inicio) en **80** y el "End Port" (Puerto de finalización) en **80**, el "Protocol" (Protocolo) en **TCP**; seleccione **Enabled (Habilitado)**; y luego haga clic en **Apply (Aplicar)**.

Port Filtering			
Start Port	End Port	Protocol	Enabled
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>
1	65535	Both	<input type="checkbox"/>

Apply

Descripciones de campos para la página avanzada de filtrado de puerto

Campo	Descripción
Start Port (Puerto de inicio)	Ingrese el número del puerto de inicio.
End Port (Puerto de finalización)	Ingrese el número del puerto de finalización.
Protocol (Protocolo)	Seleccione TCP (Protocolo de Control de Transmisión) , UDP (Protocolo de datagrama de usuario) o Both (Ambos) de la lista desplegable.
Enabled (Habilitado)	Seleccione para activar los filtros de puertos IP.

Página avanzada de redireccionamiento de puertos

Ejecute el servidor de acceso público en la red LAN especificando la asignación de puertos TCP/UDP en una PC local. Esto permite que las solicitudes entrantes en números de puertos específicos lleguen a los servidores Web, servidores FTP, servidores de correo, etc. para que se pueda obtener acceso a los mismos desde la parte pública de Internet.

Port Forwarding				
Local IP Adr	Start Port	End Port	Protocol	Enabled
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>

Números de puertos comúnmente utilizados:

- HTTP: 80
- FTP: 20, 21
- Secure Shell: 22
- Telnet: 23
- Correo electrónico SMTP: 25
- SNMP: 161

Para asignar un puerto, ingrese el rango de números de puertos para redireccionamiento local y la dirección IP a la que se debe enviar el tráfico de estos puertos. Para asignar un sólo puerto, ingrese el mismo número de puerto en las ubicaciones "start" (inicio) y "end" (finalización) para esas direcciones IP.

Página avanzada de disparadores de puertos

Configure los disparadores dinámicos para dispositivos específicos en la red LAN. Esto permite que funcionen correctamente las aplicaciones especiales que requieren números de puertos específicos con tráfico bidireccional. Las aplicaciones como videoconferencias, voz, juegos y algunas funciones de programas de mensajería pueden requerir configuraciones especiales.

Los disparadores de puertos avanzados no son puertos estáticos mantenidos abiertos todo el tiempo. Cuando el administrador de configuración detecta datos en un número de puerto IP específico definido en "Trigger Range" (Rango de disparador), los puertos resultantes definidos en "Target Range" (Rango de destino) se abren para datos entrantes o bidireccionales. Si no se detecta tráfico saliente en los puertos de "Trigger Range" (Rango de disparador) durante 10 minutos, los puertos de "Target Range" (Rango de destino) se cierran. Éste es un método más seguro para abrir puertos específicos para aplicaciones especiales (por ejemplo, programas de videoconferencias, juegos interactivos, transferencia de archivos en programas de chat, etc.) dado que se disparan dinámicamente y no se mantienen abiertos constantemente o se dejan abiertos por error a través del administrador del enrutador, ni se exponen al peligro potencial de que los hackers los descubran.

Port Triggering					
Trigger Range		Target Range		Protocol	Enable
Start Port	End Port	Start Port	End Port		
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>

Apply

Descripciones de campos para la página avanzada de disparadores de puertos

Campo	Descripción
Trigger Range (Rango de disparador):	Número de puerto de inicio del rango de disparador de puerto.
Start Port (Puerto de inicio)	Número de puerto de finalización del rango de disparador de puerto.
End Port (Puerto de finalización)	

Campo	Descripción
Target Range (Rango de destino):	Número de puerto de inicio del rango de destino de puerto.
Start Port (Puerto de inicio)	Número de puerto de finalización del rango de destino de puerto.
End Port (Puerto de finalización)	
Protocol (Protocolo)	Seleccione TCP (Protocolo de Control de Transmisión) , UDP (Protocolo de datagrama de usuario) o Both (Ambos) de la lista desplegable.
Enable (Habilitar)	Seleccione la casilla de verificación para activar los disparadores de puertos IP.

Página avanzada de host de DMZ

Especifique el destinatario predeterminado del tráfico de la red WAN que NAT no puede traducir como una PC local conocida. La zona desmilitarizada (DMZ) es una computadora o subred pequeña ubicada fuera del firewall, entre la red LAN privada interna confiable y la parte pública no confiable de Internet, que evita el acceso directo de usuarios externos a los datos privados.

Por ejemplo, puede configurar un servidor Web en un equipo de DMZ para que habilite el acceso de usuarios externos a su sitio Web sin exponer los datos confidenciales de su red.

Una zona DMZ es también útil para jugar juegos interactivos que puedan tener problemas para ejecutarse en un firewall. Puede exponer únicamente un equipo utilizado para juegos a Internet y proteger el resto de la red.

The image shows a configuration window with a blue header. Below the header, there is a label 'DMZ Address' followed by a text input field containing the IP address '192.168.0.0'. Below the input field is a button labeled 'Apply'.

Puede configurar una PC para que sea el host de DMZ. Esta configuración generalmente se utiliza para equipos que utilizan aplicaciones problemáticas que emplean números de puertos aleatorios y no funcionan correctamente con disparadores de puertos específicos o los ajustes de redireccionamiento de puertos. Si configura una PC como un host de DMZ, vuelva a establecerla en cero cuando termine con la aplicación deseada, dado que esta PC estará de hecho expuesta a la parte pública de Internet, aunque seguirá estando protegida de los ataques de negación de servicio (DoS) a través del firewall.

Configuración del host de DMZ

1. Ingrese la dirección IP del equipo.
2. Haga clic en **Apply (Aplicar)** para activar el equipo seleccionado como el host de DMZ.

Página avanzada del protocolo de información de enrutamiento

Configure los parámetros del protocolo de información de enrutamiento (RIP) relacionados con la autenticación, la máscara de subred/dirección IP de destino y los intervalos de informes. RIP identifica y utiliza automáticamente las mejores y más rápidas rutas a una determinada dirección de destino. El protocolo RIP requiere negociación de ambos lados (CMRG y CMTS) de la red. El proveedor de servicios de Internet (ISP) generalmente lo configura para que coincidan sus ajustes del sistema de terminación de cable módem (CMTS) con la configuración en el administrador de configuración (CMRG).

Nota: La mensajería de RIP sólo se envía en forma ascendente cuando se ejecuta el modo de dirección IP estática en la página de configuración básica. ¡Debe activar la dirección IP estática y luego establecer la información de red IP de la red WAN! RIP es normalmente una función que está rigurosamente controlada a través del proveedor de servicios de Internet (ISP). Las claves de autenticación y los ID de RIP se mantienen normalmente como información secreta del usuario final para evitar las configuraciones de RIP no autorizadas.

RIP Enable	<input type="checkbox"/> Enable
RIP Authentication	<input checked="" type="checkbox"/> Enable
RIP Authentication Key	<input type="text"/>
RIP Authentication Key ID	<input type="text" value="0"/>
RIP Reporting Interval	<input type="text" value="30"/> seconds
RIP Destination IP Address	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
RIP Destination IP Subnet Mask	<input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="0"/>
<input type="button" value="Apply"/>	

Descripciones de campos para la página avanzada de configuración de RIP

Campo	Descripción
RIP Enable (Habilitar RIP)	Habilita o deshabilita el protocolo RIP. RIP ayuda al enrutador a adaptarse dinámicamente a los cambios en la red. El RIP ahora se considera obsoleto ya que se han introducido nuevos protocolos de enrutamiento como el OSPF y el ISIS.
RIP Authentication (Autenticación de RIP)	Agrega una contraseña de texto plano o una clave compartida al paquete RIP para que el CPE y el enrutador inalámbrico se autenticuen.
RIP Authentication Key (Clave de autenticación de RIP)	Cifra la contraseña de texto plano que se encuentra en cada paquete RIP. Si está utilizando una clave de autenticación compartida en RIP, deberá suministrar una clave.
RIP Authentication Key ID (ID de la clave de autenticación de RIP)	Identifica la clave para crear los datos de autenticación para el paquete RIP e indica el algoritmo de autenticación.
RIP Reporting Interval (Intervalo de informe de RIP)	Determina cuánto tiempo transcurre antes de que el paquete de RIP se envíe al CPE.
RIP Destination IP Address (Dirección IP de destino de RIP)	Establece la ubicación en donde el paquete RIP se envía para actualizar la tabla de enrutamiento en su CPE.
RIP Destination IP Subnet Mask (Máscara de subred de IP de destino de RIP)	Especifica cuál CPE desea usted que reciba el paquete RIP.

7

Páginas de firewall

Use las páginas de firewall para configurar los filtros de firewall y las notificaciones de alerta de firewall. El firewall protege la red LAN de la unidad SVG1501 de los ataques y otras intrusiones de Internet. El firewall:

- Mantiene los datos de estado de cada sesión de TCP/IP en la red OSI y las capas de transporte.
- Supervisa todos los paquetes entrantes y salientes, aplica la política de firewall a cada uno, y detecta los paquetes inadecuados y los intentos de intrusión.
- Brinda registros completos para:
 - Autenticaciones de usuarios
 - Solicitudes de conexión internas y externas rechazadas
 - Creación y finalización de sesión
 - Ataques externos (detección de intrusión)

Puede configurar los filtros de firewall para establecer reglas para el uso de puertos.

Página de filtrado del contenido Web del firewall

Configure el firewall habilitando o deshabilitando varios filtros Web relacionados con el bloqueo o el otorgamiento de permiso exclusivo para diferentes tipos de datos a través del administrador de configuración de la red WAN a la red LAN.

Puede bloquear subprogramas de Java, cookies, controles de ActiveX, ventanas emergentes y proxies. La protección de firewall activa las funciones de inspección exhaustiva de paquetes (SPI) del firewall.

Web Features	
Filter Proxy	<input type="checkbox"/> Enable
Filter Cookies	<input type="checkbox"/> Enable
Filter Java Applets	<input type="checkbox"/> Enable
Filter ActiveX	<input type="checkbox"/> Enable
Filter Popup Windows	<input type="checkbox"/> Enable
Block Fragmented IP Packets	<input checked="" type="checkbox"/> Enable
Port Scan Detection	<input type="checkbox"/> Enable
IP Flood Detection	<input checked="" type="checkbox"/> Enable
Firewall Protection	<input checked="" type="checkbox"/> Enable
<input type="button" value="Apply"/>	

Seleccione cada filtro Web que desee establecer para el firewall y luego haga clic en **Apply (Aplicar)**. Los filtros Web se activarán sin la necesidad de reiniciar el administrador de configuración de la unidad SVG1501.

Nota: Por lo menos debe habilitar un filtro Web o una función para que el firewall se active. Asegúrese de que el firewall esté deshabilitado.

Página de registro local del firewall

Configure la notificación del registro de eventos del firewall en uno de los siguientes formatos:

- Alertas de correo electrónico individuales enviadas cada vez que el firewall recibe un ataque
- Registro local almacenado dentro del módem y mostrado en la página "Local Log" (Registro local)

Página de registro local del firewall

Envíe informes de ataque del firewall a un servidor SysLog estándar para que se puedan registrar múltiples instancias durante un período de tiempo. Seleccione elementos de configuración o ataque individuales para enviar al servidor SysLog para que únicamente se supervisen los elementos de interés. Puede registrar las conexiones permitidas, las conexiones bloqueadas, los tipos de ataques de Internet conocidos y los eventos de configuración del CMRG. El servidor SysLog debe estar en la misma red que la red LAN privada detrás del administrador de configuración (generalmente 192.168.0.x).

Para activar la función de supervisión de SysLog, marque todos los tipos de eventos deseados para supervisar e ingrese el último byte de la dirección IP del servidor SysLog. Normalmente, la dirección IP de este servidor SysLog está definida de modo predeterminado para que la dirección no cambie y siempre coincida con la entrada de esta página.

Send selected events

Permitted Connections

Blocked Connections

Known Internet Attacks

Product Configuration Events

to SysLog server at 192.168.0.

Apply

Descripciones de campos para la página de registro remoto del firewall

Campo	Descripción
Permitted Connections (Conexiones permitidas)	Seleccione que el servidor le envíe por correo electrónico los registros de quién se conecta a su red.
Blocked Connections (Conexiones bloqueadas)	Seleccione que el servidor le envíe por correo electrónico los registros de quién está bloqueado para conectarse a su red.
Known Internet Attacks (Ataques de Internet conocidos)	Seleccione que el servidor le envíe por correo electrónico los registros de los ataques de Internet conocidos a su red.
Product Configuration Events (Eventos de configuración de productos)	Seleccione que el servidor le envíe por correo electrónico los registros básicos de eventos de configuración de productos.
To SysLog server at 192.168.0. (Para el servidor SysLog en 192.168.0.)	Ingrese los últimos dígitos del 10 al 254 de su dirección IP del servidor SysLog.

Haga clic en **Apply (Aplicar)**.

8

Páginas de control para padres

Use las páginas de control para padres para configurar las restricciones de acceso a un dispositivo específico conectado a la red LAN de la unidad SVG1501.

Página de configuración del usuario del control para padres

Conecte a cada usuario con una regla de acceso de tiempo específico, una regla de filtrado de contenido y el inicio de sesión. También puede especificar un usuario como “usuario de confianza”, el que tendrá acceso a todo el contenido de Internet independientemente de los filtros. Puede usar la casilla de verificación “Trusted User” (Usuario de confianza) como un control para otorgar acceso completo al usuario, mientras se almacenan todas las configuraciones de filtrado para una rápida disponibilidad.

Puede habilitar cronómetros de duración de las sesiones de Internet que limitan la cantidad de tiempo para el acceso a Internet. Los usuarios deben ingresar sus contraseñas la primera vez para obtener acceso a Internet, pero no cada vez que se accede a una nueva página Web. También puede establecer el cronómetro de inactividad para que si no hay acceso a Internet por un tiempo determinado, el usuario deba iniciar sesión nuevamente.

Descripciones de campos para la página de configuración del usuario del control para padres

Campo	Descripción
Add User Button (Botón Agregar usuario)	Agregue un usuario para determinar los controles para padres para un usuario determinado.
User Settings (Configuraciones de usuario)	<p>Seleccione el usuario para el que desea modificar las restricciones de acceso.</p> <p>Seleccione Enable (Habilitar) para seleccionar el usuario.</p> <p>Haga clic en Remove User (Remover usuario) para eliminar el usuario de los controles para padres.</p>
Password (Contraseña)	Ingrese una contraseña de usuario para iniciar sesión en Internet.
Re-Enter Password (Vuelva a ingresar contraseña)	Ingrese la contraseña nuevamente para confirmación.
Trusted User (Usuario de confianza)	<p>Seleccione los usuarios que tendrán acceso completo al contenido de Internet.</p> <p>Seleccione Enable (Habilitar) para invalidar los filtros establecidos sin necesidad de desactivar las configuraciones de filtrado.</p>
Content Rule (Regla de contenido)	<p>Especifique los sitios Web a los que puede obtener acceso cada usuario.</p> <p>Seleccione White List Access Only (Únicamente acceso a la lista blanca) y luego elija un usuario de la lista desplegable.</p>
Time Access Rule (Regla de acceso de tiempo)	Establezca una regla para restringir cuándo un usuario seleccionado puede usar Internet.
Session Duration (Duración de sesión)	Establezca la cantidad de tiempo que un usuario seleccionado puede usar Internet.
Inactivity time (Tiempo de inactividad)	Establezca la cantidad de tiempo de inactividad antes de que Internet se cierre automáticamente para un usuario seleccionado.
Trusted Computers (Equipos de confianza)	<p>Ingrese la dirección MAC del CPE para que el CPE pueda obtener acceso a Internet sin ser censurado por el control para padres.</p> <p>Cuando haya finalizado, haga clic en Add (Agregar).</p>

Haga clic en **Apply (Aplicar)** para activar y guardar cualquier cambio que haya realizado.

Página de configuración básica del control para padres

Establezca las reglas para bloquear los tipos de contenido de Internet y determinados sitios Web.

Parental Control Activation
This box must be checked to turn on Parental Control
 Enable Parental Control
Apply

Content Policy Configuration
Add New Policy
1. Default Remove Policy
Keyword List: anonymizer
Blocked Domain List: anonymizer.com
Allowed Domain List
Add Remove Add Remove Add Remove

Override Password
If you encounter a blocked website, you can override the block by entering the following password
Password:
Re-Enter Password:
Access Duration: 30
Apply

Luego de cambiar la configuración de “Parental Control” (Control para padres), haga clic en el botón **Apply (Aplicar)**, **Add (Agregar)** o **Remove (Quitar)** que corresponda.

Haga clic en **Refresh (Actualizar)** en la ventana de su explorador Web para ver las configuraciones actuales.

Página de filtrado de hora del día del control para padres

Bloquee todo el tráfico de Internet de y hacia dispositivos específicos en la red de su unidad SVG1501 según la configuración de día y hora. Puede bloquear el tráfico de Internet para todo el día o para ciertas horas del día para usuarios específicos. Puede agregar hasta 30 categorías de ocho caracteres (nombres de filtros) con distintas configuraciones de día y hora. Puede ingresar un nombre para cada filtro de hora en el campo **Add New Policy (Agregar nueva política)**.

Aplique los filtros de hora para acceso a Internet limitado para cada usuario en el campo **Time Access Rule (Regla de acceso de tiempo)** en la [Página de configuración del usuario del control para padres](#).

Luego de crear cada categoría, haga clic en **Apply (Aplicar)** en la parte inferior de la página para almacenar y activar las configuraciones. Los mismos nombres de categoría para el bloque de perfiles aparecen en la página “Parental Control User Setup” (Configuración del usuario del control para padres) en la sección “Time Access Rule” (Regla de acceso de tiempo) donde se le puede asignar un máximo de cuatro categorías de manera simultánea a cada usuario.

Página del registro local del control para padres

Genere un registro de eventos que muestre una lista actualizada de las 30 violaciones de acceso más recientes al control para padres, entre ellas:

- Si el acceso a Internet del usuario se bloqueó (filtro de tiempo)
- Si se detectó una palabra clave bloqueada en la URL
- Si se detectó un dominio bloqueado en la URL
- Si el servicio de búsquedas en línea detecta que la URL se cae frente a una categoría bloqueada

9

Páginas inalámbricas

Para configurar su red LAN inalámbrica (WLAN), haga clic en cualquier opción del submenú inalámbrico para ver o cambiar la información de configuración para dicha opción. El cifrado WPA o WPA2 brinda un nivel más alto de seguridad que el cifrado WEP, pero es posible que las tarjetas de cliente inalámbrico más antiguas no sean compatibles con los métodos de cifrado WPA o WPA2.

Página de radio inalámbrico 802.11

Configure los parámetros de radio inalámbrico, incluidos los números de canal y país actuales.

Wireless Interfaces: Motorola (00:90:4C:A3:09:42)	
Wireless	Enabled
Country	UNITED STATES
Output Power	100%
Channel	1
Current : 1	
Apply	Restore Wireless Defaults

Descripciones de campos para la página de radio inalámbrico 802.11

Campo	Descripción
Wireless Interfaces (Interfaces inalámbricas)	Muestra la dirección MAC de la tarjeta inalámbrica instalada. No se puede configurar.
Wireless (Redes inalámbricas)	Muestra si la red inalámbrica está habilitada o deshabilitada
Country (País)	Restringe el conjunto de canales según los requisitos reglamentarios del país. Éste es un campo que sólo se puede visualizar.
Output Power (Potencia de salida)	Define un porcentaje de la potencia de salida de la capacidad máxima de hardware.
Channel (Canal)	Selecciona el canal para la operación del punto de acceso (AP). La lista de canales disponibles depende del país designado. Para este campo, el canal seleccionado en los clientes inalámbricos en su red WLAN debe ser el mismo que se seleccionó en la unidad SVG1501.

Página de red principal inalámbrica 802.11

Configure su red inalámbrica principal.

Descripciones de campos para la página de red principal inalámbrica 802.11

Campo	Descripción
Primary Network (Red principal)	Cuando está en Enabled (Habilitada) , transmite los marcos guía con el identificador de conjunto de servicios (SSID) de la red principal.
Network Name [SSID] (Nombre de red [SSID])	Establece el nombre de red (SSID) de la red inalámbrica principal usando la cadena de caracteres 1-32 ASCII.
Closed Network (Red cerrada)	En una red cerrada, los usuarios escriben el SSID en la aplicación cliente en lugar de seleccionar el SSID de una lista.
WPA	Habilita o deshabilita el cifrado de acceso Wi-Fi protegido.
WPA-PSK	Habilita o deshabilita una frase clave local de WPA previamente compartida.
WPA2	Habilita o deshabilita el cifrado de acceso Wi-Fi protegido 2.
WPA2-PSK	Habilita o deshabilita una frase clave local de WPA2 previamente compartida.
WPA/WPA2 Encryption (Cifrado WPA/WPA2)	Establece el modo de cifrado en: TKIP, AES, o TKIP + AES. AES.

Campo	Descripción
WPA Pre-Shared Key (Clave de WPA previamente compartida) Show Key (Mostrar clave)	Establece la clave de WPA previamente compartida (PSK); ya sea una cadena de caracteres 8-63 ASCII o un número de 64 dígitos hexadecimales. Esto se especifica cuando el método de autenticación de red es WPA-PSK. Show Key (Mostrar clave): muestra la clave de WPA previamente compartida.
RADIUS Server (Servidor RADIUS)	Establece la dirección IP del servidor RADIUS para usar durante la autenticación del cliente utilizando el formato decimal separado por puntos (xxx.xxx.xxx.xxx).
RADIUS Port (Puerto RADIUS)	Establece el número de puerto UDP (protocolo de datagrama de usuario) del servidor RADIUS; el valor predeterminado es 1812.
RADIUS Key (Clave RADIUS)	Establece el secreto compartido para la conexión RADIUS; la clave es una cadena de 0 a 255 caracteres ASCII.
Group Key Rotation Interval (Intervalo de rotación de clave de grupo)	Establece el intervalo de cambio de clave de grupo de WPA en segundos. Configúrelo en cero para deshabilitar el cambio de clave periódico.
WPA/WPA2 Re-auth Interval (Intervalo de reautenticación de WPA/WPA2)	Establece la cantidad de tiempo que el enrutador inalámbrico puede esperar antes de restablecer la autenticación con el CPE.
WEP Encryption (Cifrado WEP)	Habilita o deshabilita el cifrado de privacidad equivalente cableado.
Shared Key Authentication (Autenticación de clave compartida)	Envía una solicitud de autenticación al punto de acceso. Luego, el punto de acceso envía un texto de desafío al CPE. El CPE cifra el texto de desafío y lo envía al punto de acceso. El punto de acceso descifra y compara el mensaje con el texto de desafío original. Si son iguales, el punto de acceso permite que el CPE se conecte; si no coinciden, el punto de acceso no permite que el CPE se conecte.
802.1x Authentication (Autenticación 802.1x)	Usa una autenticación más sólida que WEP y se puede combinar.
Network Key 1 – 4 (Clave de red 1 – 4)	Establece las claves WEP estáticas cuando el cifrado WEP está habilitado. <ul style="list-style-type: none"> • Ingrese cinco caracteres ASCII o 10 dígitos hexadecimales para una clave de 64 bits. • Ingrese 13 caracteres ASCII o 26 dígitos hexadecimales para una clave de 128 bits. Cuando el cifrado WPA y el cifrado WEP están habilitados, únicamente las claves 2 y 3 están disponibles para el cifrado WEP.

Campo	Descripción
Current Network Key (Clave de red actual)	Selecciona la clave de cifrado (transmisión) cuando está habilitado el cifrado WEP.
PassPhrase (Frase clave)	Establece el texto que se utilizará en la generación de la clave WEP.

Página avanzada inalámbrica 802.11

Configure las tasas de datos y los umbrales de Wi-Fi.

54g™ Mode	54g LRS
Basic Rate Set	Default
54g™ Protection	Auto
XPress™ Technology	Disabled
Afterburner™ Technology	Disabled
Rate	Auto
Output Power	100%
Beacon Interval	100
DTIM Interval	1
Fragmentation Threshold	2346
RTS Threshold	2347
Apply	

Descripciones de campos para la página avanzada inalámbrica 802.11

Campo	Descripción
54g™ Mode (Modo 54g™)	<p>Establece estos modos de red:</p> <ul style="list-style-type: none"> 54g Auto 54g Performance 54g LRS 802.11b only <p>“54g Auto” (54g automático) acepta clientes 54g, 802.11g y 802.11b pero optimiza el rendimiento según el tipo de clientes conectados. “54g Performance” (54g de rendimiento) acepta únicamente a clientes 54g y ofrece el rendimiento general más alto; las redes que se acerquen a 802.11b pueden sufrir una merma en su rendimiento. “54g de compatibilidad con tasa limitada” interactúa con la variedad más amplia de clientes 54g, 802.11g y 802.11b. 802.11b sólo acepta a los clientes 802.11b.</p>

Campo	Descripción
Basic Rate Set (Tasa básica fija)	Determina que tasas se anuncian como tasas básicas. La opción "Default" (Predeterminada) utiliza los valores predeterminados del controlador. La opción "All" (Todos) establece todas las tasas disponibles como tasas básicas.
54g™ Protection (Protección 54g™)	Mejora el rendimiento en el modo "Auto" (Automático) a través de la protección RTS/CTS en redes 802.11g + 802.11b combinadas. Desactive la protección para maximizar el rendimiento de 802.11g en la mayoría de las condiciones.
XPress™ Technology (Tecnología XPress™)	Mejora el rendimiento inalámbrico y la eficiencia cuando hay redes inalámbricas combinadas en el área circundante desde redes 802.11a/b/g.
Afterburner™ Technology (Tecnología Afterburner™)	Mejora el estándar Wi-Fi 802.11g al aumentar el rendimiento en un 40 por ciento.
Rate (Tasa)	Establece la tasa de transmisión del AP en una velocidad determinada. "Auto" (Automático) ofrece el mejor rendimiento en casi todas las situaciones.
Output Power (Potencia de salida)	Define la potencia de salida como un porcentaje de la capacidad máxima de hardware.
Beacon Interval (Intervalo de la guía)	Establece el intervalo de la guía del AP. El valor predeterminado es 100, que es adecuado para casi todas las aplicaciones.
DTIM Interval (Intervalo de DTIM)	Establece el intervalo de activación de los clientes en el modo "Power Save" (Ahorro de energía). Cuando un cliente se ejecuta en el modo de ahorro de energía, los valores más bajos de la unidad SVG1501 ofrecen un mayor rendimiento pero una menor vida útil de la batería del cliente, y los valores más altos ofrecen menor rendimiento pero mayor vida útil de la batería del cliente.
Fragmentation Threshold (Umbral de fragmentación)	Establece el umbral de fragmentación. Los paquetes que superen este umbral se fragmentarán en paquetes más pequeños que el umbral antes de su transmisión.
RTS Threshold (Umbral de RTS)	Establece el umbral de RTS. Los paquetes que superen este umbral ocasionarán el cambio de RTS/CTS en AP a fin de reservar el medio inalámbrico antes de la transmisión de paquetes.

Página de control del acceso inalámbrico 802.11

Configure el control de acceso para el AP y el estado en los clientes conectados.

Descripciones de campos para la página de control del acceso inalámbrico 802.11

Campo	Descripción
Wireless Interface (Interfaz inalámbrica)	Muestra la dirección MAC de la tarjeta inalámbrica instalada. No se puede configurar.
MAC Restrict Mode (Modo de restricción por MAC)	Selecciona si se les permite o deniega el acceso inalámbrico a los clientes inalámbricos con la dirección MAC especificada. Seleccione Disabled (Deshabilitado) para permitir todos los clientes.
MAC Address (Dirección MAC)	Lista las direcciones MAC de los clientes inalámbricos a las que se les permite o deniega el acceso inalámbrico según la configuración de "Restrict Mode" (Modo de restricción). Los formatos de dirección MAC de entrada válidos son XX:XX:XX:XX:XX:XX y XX-XX-XX-XX-XX-XX.
Connected Clients (Clientes conectados)	Lista los clientes inalámbricos conectados. Cuando un cliente se conecta, se lo agrega a la lista; cuando abandona la red, se lo quita de la lista. La antigüedad es la cantidad de tiempo que transcurrió desde que se transmitieron o recibieron datos desde el cliente.

Página de multimedia inalámbrica 802.11

Configure la calidad de servicio (QoS) de multimedia Wi-Fi.

WMM Support	On						
No-Acknowledgement	Off						
Power Save Support	On						
Apply							
EDCA AP Parameters:	CWmin	CWmax	AIFS	TXOP(b) Limit (usec)	TXOP(a/g) Limit (usec)	Admission Control	Discard Oldest First
AC_BE	15	63	3	0	0		Off
AC_BK	15	1023	7	0	0		Off
AC_VI	7	15	1	6016	3008		Off
AC_VO	3	7	1	3264	1504		Off
EDCA STA Parameters:							
AC_BE	15	1023	3	0	0		
AC_BK	15	1023	7	0	0		
AC_VI	7	15	2	6016	3008		
AC_VO	3	7	2	3264	1504		
Apply							

Descripciones de campos para la página de multimedia inalámbrica 802.11

Campo	Descripción
WMM Support (Compatibilidad con multimedia Wi-Fi)	<p>Establece la compatibilidad con multimedia Wi-Fi en "Auto" (Automático), On (Activada) o Off (Desactivada).</p> <p>Si está habilitada (Auto u On), se incluye el elemento de información de WME en los marcos guía.</p>
No-Acknowledgement (No reconocimiento)	<p>Establece la compatibilidad con el estado de no reconocimiento en "On" (Activada) u "Off" (Desactivada).</p> <p>Cuando está activada, no se transmiten los reconocimientos de datos.</p>
Power Save Support (Compatibilidad con ahorro de energía)	<p>Establece la compatibilidad con el ahorro de energía en "On" (Activado) u "Off" (Desactivado).</p> <p>Si está activado, el AP pone en cola a los paquetes de STA que estén en modo de ahorro de energía. Los paquetes en cola se transmiten cuando el STA notifica al AP que ha salido del modo de ahorro de energía.</p>
EDCA AP Parameters (Parámetros EDCA del AP)	<p>Especifica los parámetros de transmisión del tráfico transmitido del AP al STA en cuatro categorías de acceso:</p> <p>"Admission control" (Control de admisión) especifica si este control se aplica a las categorías de acceso.</p> <p>"Discard Oldest First" (Descartar las más antiguas primero) especifica la política de descarte de las colas. "On" (Activado) descarta la más antigua primero; "Off" (Desactivado) descarta la más nueva primero.</p>

Campo	Descripción
EDCA STA Parameters (Parámetros EDCA del STA)	Especifica los parámetros de transmisión del tráfico transmitido del STA al AP en cuatro categorías de acceso.

Página de extensión inalámbrica 802.11

Habilita la extensión inalámbrica.

Descripciones de campos para la página de extensión inalámbrica 802.11

Campo	Descripción
Wireless Bridging (Extensión inalámbrica)	Habilite o deshabilite la extensión inalámbrica.
Remote Bridges (Extensiones inalámbricas)	Cree una tabla de direcciones MAC de extensiones remotas autorizadas para establecer una extensión inalámbrica. Puede conectar hasta cuatro extensiones remotas. Por lo general, debe ingresar la dirección MAC de su AP en la extensión remota.

Configuración de su red LAN inalámbrica

Puede utilizar la unidad SVG1501 como un punto de acceso para una red LAN inalámbrica (WLAN) sin cambiar las configuraciones predeterminadas.

PRECAUCIÓN: Evite el acceso o uso indebido no autorizado habilitando la seguridad inalámbrica una vez que su red WLAN esté en funcionamiento. Las configuraciones predeterminadas no ofrecen seguridad inalámbrica.

Para habilitar la seguridad para su red WLAN:

- Cifre las transmisiones de la red LAN inalámbrica
- Restrinja el acceso inalámbrico a la red LAN para evitar intrusiones no autorizadas a la red WLAN a través de la [Página de control del acceso inalámbrico 802.11](#)

PRECAUCIÓN: No proporcione nunca su SSID, WPA o frase clave WEP, o su clave WEP a ninguna persona que no esté autorizada para usar su red WLAN.

No intente configurar la unidad SVG1501 a través de una conexión inalámbrica.

Conecte por lo menos un equipo al puerto Ethernet de la unidad SVG1501.

Configure cada cliente inalámbrico (estación) para obtener acceso a la unidad SVG1501.

Ubique los componentes inalámbricos lejos de las ventanas. Esto disminuye la intensidad de la señal fuera del área deseada.

Cifrado de las transmisiones de la red LAN inalámbrica

Para evitar la visualización no autorizada de los datos transmitidos a través de su red WLAN, debe cifrar sus transmisiones inalámbricas. Elija una de las siguientes opciones:

Cifrado de las transmisiones de la red LAN inalámbrica

Configure en la unidad SVG1501	Requerido en cada cliente inalámbrico
<p>Si todos sus clientes inalámbricos son compatibles con el acceso Wi-Fi protegido (WPA), Motorola recomienda que configure WPA en la unidad SVG1501</p>	<p>Si utiliza una frase clave local previamente compartida (WPA-PSK), debe configurar la misma frase clave en la unidad SVG1501 y en cada cliente inalámbrico. Las configuraciones hogareñas y para pequeñas oficinas generalmente utilizan una frase clave local.</p>
<p>De lo contrario, configure WEP en la unidad SVG1501</p>	<p>Debe configurar la misma clave WEP en la unidad SVG1501 y en cada cliente inalámbrico.</p>

Motorola recomienda utilizar WPA en lugar de WEP si todos sus clientes inalámbricos son compatibles con el cifrado WPA. Ventajas de WPA:

- Cifrado más sólido y seguro
- Autenticación para garantizar que sólo los usuarios autorizados puedan registrarse en su red WLAN
- Configuración más fácil
- Algoritmo estándar en todos los productos compatibles para generar una clave de una frase clave de textual
- Incorporación al nuevo estándar de red inalámbrica IEEE 802.11i


Para las nuevas redes LAN inalámbricas, Motorola recomienda comprar adaptadores cliente que sean compatibles con el cifrado WPA.

Instalación de clientes inalámbricos

Nota: Use el CD-ROM de instalación de la unidad SVG1501 para establecer la seguridad del cliente. La contraseña está ubicada en la etiqueta de la puerta de enlace.

Para cada equipo cliente inalámbrico, siga las instrucciones suministradas con el adaptador y los pasos que figuran a continuación para instalar el adaptador inalámbrico:

1. Inserte el CD-ROM para el adaptador en la unidad de CD-ROM en el cliente.
2. Instale el software del dispositivo desde el CD.
3. Inserte el adaptador en la ranura PCMCIA o PCI, o conéctelo al puerto USB.
4. Configure el adaptador para obtener automáticamente una dirección IP.

En una PC con Wireless Client Manager (Administrador de cliente inalámbrico) instalado, aparece el ícono  en la barra de tareas de Windows. Haga doble clic en el ícono para iniciar la herramienta. Es posible que deba seguir estos pasos para utilizar un equipo cliente inalámbrico para obtener acceso a Internet:

Configuración de clientes inalámbricos

Si:	Debe hacer lo siguiente en cada cliente:
Configuró WPA en la unidad SVG1501	Configure un cliente inalámbrico para WPA o WPA2
Configuró WEP en la unidad SVG1501	Configure un cliente inalámbrico para WEP
Configuró el nombre de la red inalámbrica en la unidad SVG1501	Configure un cliente inalámbrico con el nombre de la red (SSID)
Configuró una lista de control de acceso MAC en la unidad SVG1501	No necesita configurar el cliente

Instalación de un cliente inalámbrico para WPA

Si habilitó WPA y estableció una frase clave PSK configurando WPA en la unidad SVG1501, debe configurar la misma frase clave en cada cliente inalámbrico. La unidad SVG1501 no puede autenticar un cliente si:

- WPA está habilitado en la unidad SVG1501 pero no en el cliente
- La frase clave del cliente no coincide con la frase clave PSK de la unidad SVG1501

PRECAUCIÓN: No suministre nunca la frase clave PSK a ninguna persona no autorizada a utilizar su red WLAN.

Configuración de un cliente inalámbrico para WEP

Si habilitó WEP y estableció una clave configurando WEP en la unidad SVG1501, debe configurar la misma clave WEP en cada cliente inalámbrico. La unidad SVG1501 no puede autenticar un cliente si:

- La autenticación de clave compartida está habilitada en la unidad SVG1501 pero no en el cliente
- La clave WEP del cliente no coincide con la clave WEP de la unidad SVG1501

Para todos los adaptadores inalámbricos, debe ingresar una clave WEP de 64 bits o 128 bits generada por la unidad SVG1501.

PRECAUCIÓN: No suministre nunca la clave WEP a ninguna persona no autorizada a utilizar su red WLAN.

Configuración de un cliente inalámbrico con el nombre de la red (SSID)

Luego de especificar el nombre de la red en la página básica inalámbrica, muchos adaptadores o tarjetas inalámbricos analizan automáticamente un punto de acceso, como la unidad SVG1501 y la tasa de datos y canales apropiados. Si su tarjeta requiere que inicie manualmente el análisis de un punto de acceso, siga las instrucciones en la documentación suministrada con la tarjeta. Debe ingresar el mismo SSID en el ajuste de configuración inalámbrica del dispositivo para que se comunique con la unidad SVG1501.

10

Páginas de VPN

Las páginas de **VPN (Red privada virtual)** permiten que configure y administre los túneles de VPN.

Puede hacer clic en cualquier opción del submenú VPN para ver o cambiar la información de configuración para dicha opción.

Página básica de VPN

Habilite los protocolos de VPN y administre los túneles de VPN.

L2TP / PPTP				
L2TP Server	Disabled ▾			
PPTP Server	Disabled ▾			
Configure				
IPsec				
IPsec Endpoint	Enabled ▾			
#	Name	Status	Control	Configure
1		NOT Connected	N/A	Edit Delete
2		NOT Connected	N/A	Edit Delete
Add New Tunnel...				

Campo	Descripción
L2TP Server (Servidor L2TP)	Habilite o deshabilite el protocolo de túnel del nivel 2
PPTP Server (Servidor PPTP)	Habilite o deshabilite el protocolo de punto a punto
IPsec Endpoint (Terminal IPsec)	Habilite o deshabilite el protocolo de seguridad de Internet
Add New Tunnel (Agregar nuevo túnel)	Cree una nueva configuración de túnel y agréguela a la tabla. Haga clic en Edit (Editar) para agregar el nombre y las características del túnel.

Página IPsec de VPN

Puede configurar múltiples túneles de VPN para diversos equipos cliente y almacenar diferentes túneles, pero no puede habilitarlos para que sea más fácil utilizarlos con conexiones y/o equipos cliente que no se utilicen con regularidad.

Para cada configuración de túnel que almacene, los parámetros IPsec exclusivos se almacenan a través de la sección "IPsec Settings" (Configuraciones de IPsec) en la parte inferior de la página. Haga clic en **Show Advanced Settings (Mostrar configuraciones avanzadas)** en la parte inferior de la página para mostrar las funciones avanzadas que controlan la administración de claves IPSEC y la negociación con la terminal remota.

Tunnel	1	Delete Tunnel
Name	<input type="text"/>	Add New Tunnel
	Disabled	Apply
Local endpoint settings		
Address group type	IP subnet	
Subnet	192.168.0.0	
Mask	255.255.255.0	
Identity type	IP address	
Identity	<input type="text"/>	
Remote endpoint settings		
Address group type	IP subnet	
Subnet	0.0.0.0	
Mask	255.255.255.0	
Identity type	IP address	
Identity	<input type="text"/>	
Network address type	IP address	
Remote Address	0.0.0.0	
IPsec settings		
Pre-shared key	EnterAKey	
Phase 1 DH group	Group 1 (768 bits)	
Phase 1 encryption	DES	
Phase 1 authentication	MD5	
Phase 1 SA lifetime	28800	seconds
Phase 2 encryption	DES	
Phase 2 authentication	MD5	
Phase 2 SA lifetime	3600	seconds
Show Advanced Settings		
Apply		

Campo	Descripción
Tunnel (Túnel)	Configure cada túnel de forma individual. Los túneles preestablecidos se detallan por su nombre preestablecido.
Name (Nombre)	<p>Asigne un nombre genérico para un grupo de configuraciones de un túnel.</p> <p>Luego de ingresar por primera vez el nombre del túnel correspondiente, haga clic en Add New Tunnel (Agregar nuevo túnel) para crear un título para las configuraciones del túnel seleccionadas en la lista desplegable Tunnel (Túnel). Si no asigna un nombre, se numerarán los túneles de forma secuencial.</p>
Enable drop-down (Lista desplegable Habilitar)	<p>Luego de asignar un nombre y configurar un túnel de VPN, puede almacenarlo como deshabilitado o habilitado a través de la lista desplegable "Enable/Disable" (Habilitar/Deshabilitar). Haga clic en Apply (Aplicar) para alternar "Enable/Disable" (Habilitar/Deshabilitar).</p>
Local Endpoint Settings (Configuraciones de terminales locales) Address group type (Tipo de grupo de direcciones)	<p>Asígnele al grupo de acceso de VPN local uno de los siguientes tipos de grupos:</p> <p>Single IP address (Dirección IP única): si se trata de un solo equipo, ingrese la dirección IP correspondiente</p> <p>IP address range (Rango de dirección IP): si se trata de un rango reducido de equipos, ingrese las direcciones IP de inicio y finalización del grupo de direcciones IP consecutivas que tendrán acceso al túnel de VPN</p> <p>IP Subnet (Subred IP): si se trata de una subred/red completa, ingrese la subred y máscara para el rango de dirección IP y la subred IP. Ingrese las direcciones IP de inicio y finalización del grupo de direcciones IP consecutivas que tendrán acceso al túnel de VPN.</p>
Identity Type (Tipo de identidad)	<p>Defina que el tipo de identidad de terminal local use automáticamente la dirección IP de la red WAN del enrutador o como una dirección IP definida por el usuario, el nombre de dominio completo (FQDN) o la dirección de correo electrónico. La terminal remota lo utiliza para identificar el punto de finalización e intercambio de VPN.</p> <p>La configuración de la terminal de VPN remota del otro lado del túnel debe coincidir con esta configuración.</p>
Identity (Identidad)	<p>Ingrese la cadena de identidad.</p> <p>En caso de una dirección IP, ingrese <i>x.x.x.x</i>.</p> <p>En caso de FQDN, ingrese <i>sudominio.com</i></p> <p>En caso de una dirección de correo electrónico, ingrese <i>sunombre@sudominio.com</i></p> <p>La configuración de la terminal de VPN remota del otro lado del túnel debe coincidir con esta configuración.</p>

Campo	Descripción
Remote Endpoint Settings (Configuraciones de terminales remotas) Address group type (Tipo de grupo de direcciones)	<p>Asígnele al grupo de acceso de VPN remota uno de los siguientes tipos de grupos:</p> <p>Single IP address (Dirección IP única): si se trata de un solo equipo, ingrese la dirección IP correspondiente</p> <p>IP address range (Rango de dirección IP): si se trata de un rango reducido de equipos, ingrese las direcciones IP de inicio y finalización del grupo de direcciones IP consecutivas que tendrán acceso al túnel de VPN</p> <p>IP Subnet (Subred IP): si se trata de una subred/red completa, ingrese la subred y máscara</p> <p>Si se trata de un rango de direcciones IP y subred IP, ingrese las direcciones IP de inicio y finalización del grupo de direcciones IP consecutivas que tendrán acceso al túnel de VPN.</p> <p>La configuración de la terminal de VPN local del otro lado del túnel debe coincidir con esta configuración.</p>
Identity type (Tipo de identidad)	<p>Defina que el tipo de identidad de terminal remota use automáticamente la dirección IP de la terminal remota o como una dirección IP definida por el usuario, el nombre de dominio completo (FQDN) o la dirección de correo electrónico. Ésta es la identidad que la terminal remota utiliza para identificar el punto de finalización e intercambio de VPN.</p> <p>La configuración de la terminal de VPN local del otro lado del túnel debe coincidir con esta configuración.</p>
Identity (Identidad)	<p>Ingrese la cadena de identidad:</p> <p>En caso de una dirección IP, ingrese x.x.x.x.</p> <p>En caso de FQDN, ingrese <i>sudominio.com</i></p> <p>En caso de una dirección de correo electrónico, ingrese <i>sunombre@sudominio.com</i></p> <p>La configuración de la terminal de VPN local del otro lado del túnel debe coincidir con esta configuración.</p>
Network address type (Tipo de dirección de red)	<p>Seleccione el tipo de dirección de red WAN de la terminal remota: Dirección IP o nombre de dominio completo (FQDN)</p>
Remote Address (Dirección remota)	<p>Ingrese la dirección IP de la terminal remota o su FQDN.</p>
IPsec Settings (Configuraciones de IPsec)	<p>Asocie una de las dos fases de la asociación de seguridad (SA) al túnel de VPN. La fase 1 crea una SA de intercambio de claves de Internet (IKE). Luego de finalizada la fase 1, la fase 2 crea una o más SA de IPSEC, que se utilizan posteriormente para codificar las sesiones de IPSEC.</p>

Campo	Descripción
Pre-shared key (Clave previamente compartida)	Ingrese el campo "Pre-shared Key" (Clave previamente compartida) si un lado del túnel de VPN está usando un identificador de firewall único (o clave previamente compartida).
Phase 1 DH group (Fase 1 - Grupo de DH)	<p>Seleccione uno de los grupos de Diffie-Hellman: 768 bits, 1024 bits o 1536 bits.</p> <p>Diffie-Hellman es una técnica criptográfica que utiliza claves públicas y privadas para el cifrado y descifrado. Cuanto más alto sea el número de bits, más seguro será el cifrado. Opciones: Grupo 1 (768 bits), Grupo 2 (1024 bits) o Grupo 5 (1536 bits).</p>
Phase 1 encryption (Fase 1 - Cifrado)	<p>Proteja la conexión de VPN entre terminales con el cifrado: DES, 3DES, AES-128, AES-192 o AES-256.</p> <p>Seleccione cualquier opción de cifrado pero debe coincidir con las terminales remotas. Las configuraciones de cifrado más utilizadas son 3DES y AES.</p>
Phase 1 authentication (Fase 1 - Autenticación)	<p>Establezca "Authentication" (Autenticación), otro nivel de seguridad, en SHA o MD5.</p> <p>Motorola recomienda SHA ya que es más seguro, pero puede utilizar cualquier tipo de autenticación siempre y cuando el otro extremo del túnel de VPN use el mismo método.</p>
Phase 1 SA lifetime (Fase 1 - Duración de SA)	<p>Especifique la duración de las claves rotativas individuales.</p> <p>Ingrese el número de segundos que la clave permanecerá hasta que se vuelva a negociar entre cada terminal. La configuración predeterminada es 28.000 segundos.</p> <p>Una duración menor es por lo general más segura, dado que le proporciona al atacante una cantidad menor de tiempo para intentar violar la clave. Sin embargo, la negociación de claves consume ancho de banda, de modo que el rendimiento de la red se ve sacrificado con tiempos más cortos. Las entradas, por lo general, se expresan en milésimas o decenas de milésimas de segundos.</p>

Página L2TP/PPTP de VPN

Configure las opciones de servidor L2TP y PPTP.

PPP Address Range	
Start	10 . 0 . 0 . 1
End	10 . 0 . 0 . 254
PPP Security	
MPPE Encryption	Enabled
Apply	
Users	
Username	<input type="text"/>
Password	<input type="password"/>
Confirm Password	<input type="password"/>
Add	
User List	
User list is empty.	
L2TP Server	
Preshared Phrase	<input type="text"/>
Apply	

Campo	Descripción
PPP Address Range (Rango de direcciones PPP) Start (Inicio) End (Finalización)	Especifique el rango de direcciones IP de inicio y finalización para que cuando el túnel esté configurado, el lado del cliente y del servidor obtenga su dirección IP desde este rango especificado.
PPP Security (Seguridad de PPP) MPPE Encryption (Cifrado de MPPE)	Habilite o deshabilite el cifrado de punto a punto de Microsoft (MPPE). Es un tipo de cifrado de vínculos que se usa en PPTP. Esto significa que se cifran los datos enviados a través de este túnel.
Username (Nombre de usuario)	Autentica el túnel que se creó entre el cliente y el servidor.
Password (Contraseña)	Ingrese una contraseña de usuario para la autenticación.
Confirm Password (Confirmar contraseña)	Ingrese la contraseña nuevamente para confirmación.
Preshared Phrase (Fase previamente compartida)	Autentica el servidor del protocolo de túnel del nivel 2 (L2TP).

Página del registro de eventos de VPN

Vea el registro de eventos de VPN, que muestra un historial de las conexiones y la actividad de VPN en orden cronológico y la dirección IP de las terminales remotas y locales en el túnel.

Time	Description
Event log is empty.	

Refresh Clear

- Haga clic en **Refresh (Actualizar)** para actualizar la tabla "Event Log" (Registro de eventos) para que muestre cualquier cambio realizado desde que se cargó por última vez la página Web.
- Haga clic en **Clear (Borrar)** para borrar el contenido actual de la tabla de registro. Sólo aparecerán los datos más recientes.

11

Páginas de MTA

Use Internet para realizar llamadas telefónicas. El adaptador de terminal multimedia (MTA) es compatible con las funciones telefónicas básicas, como llamada tripartita, correo de voz y transmisiones de fax.

Página de estado de MTA

Muestra el estado de inicialización de MTA.

Startup Procedure	
Task	Status
Telephony DHCP	Completed
Telephony Security	Disabled
Telephony TFTP	Completed
Telephony Call Server Registration	L1: Operational / L2: Operational
Telephony Registration Complete	Pass With Warnings
MTA Line State	
Line 1	On-Hook
Line 2	On-Hook

Página de DHCP de MTA

Muestra la información de concesión de DHCP de MTA.

Lease Paramteres	
FQDN	mta001a66080b06.swdev.net
IP Address/Submask	206.19.81.247 / 255.255.255.0
Gateway	206.19.81.1
Bootfile	tftp://sbvprov3.swdev.net/001A66080B06.bin
Primary DNS	198.102.87.133
Secondary DNS	0.0.0.0
Lease Timers	
Lease Time Remaining	D: 00 H: 00 M: 27 S: 58
Rebind Time Remaining	D: 00 H: 00 M: 12 S: 58
Renew Time Remaining	D: 00 H: 00 M: 01 S: 43
PacketCable DHCP Option 122	
SNMP Entity (Sub-option 3)	sbvprov3.swdev.net
Kerberos Realm (Sub-option 6)	
Provisioning Timer (Sub-option 8)	

Página de QoS de MTA

Esta página muestra los parámetros de calidad de servicio (QoS) de MTA.

Error Codewords				
Unerrored Codewords		128653228		
Correctable Codewords		0		
Uncorrectable Codewords		0		
Payload Header Suppression				
PHS Status		ON		
Service Flows				
SFID	Service Class Name	Direction	Primary Flow	Packets
3543		Upstream	No	23806
3544		Downstream	No	0
4133		Upstream	No	6
4134		Downstream	No	0

Página de suministro de MTA

Esta página muestra los detalles de suministro de MTA sobre la conexión telefónica de voz por Internet (VoIP) de su unidad SVG1501.

MTA Config File	
Filename	ftp://sbvprov3.swdev.net/001A66080B06.bin
Contents	<pre> MTA Config File Contents ===== 1.3.6.1.4.1.4491.2.2.1.1.1.7.0.1 1.3.6.1.2.1.2.2.1.7.9.1 1.3.6.1.2.1.2.2.1.7.10.1 1.3.6.1.4.1.4491.2.2.2.1.1.10.0.2 1.3.6.1.4.1.4491.2.2.2.1.1.8.0.24 1.3.6.1.4.1.4491.2.2.2.1.1.9.0.40 1.3.6.1.4.1.4491.2.2.2.1.1.12.0.2427 1.3.6.1.4.1.4491.2.2.2.1.1.6.0.FFC00000 1.3.6.1.4.1.4491.2.2.2.1.1.6.0.FFC00000 1.3.6.1.4.1.4491.2.2.2.1.1.7.0.FFC00000 1.3.6.1.4.1.4491.2.2.2.1.2.1.1.18.9.10 1.3.6.1.4.1.4491.2.2.2.1.2.1.1.18.10.10 1.3.6.1.4.1.4491.2.2.2.1.2.1.1.27.9.1 1.3.6.1.4.1.4491.2.2.2.1.2.1.1.27.10.1 1.3.6.1.4.1.4491.2.2.2.1.2.1.1.28.9.8 1.3.6.1.4.1.4491.2.2.2.1.2.1.1.28.10.8 1.3.6.1.4.1.4491.2.2.2.1.2.1.1.2.9.2427 1.3.6.1.4.1.4491.2.2.2.1.2.1.1.2.10.2427 1.3.6.1.4.1.4491.2.2.2.1.2.1.1.1.9.SBVPROV3-CA.SWDEV.NET 1.3.6.1.4.1.4491.2.2.2.1.2.1.1.1.10.SBVPROV3-CA.SWDEV.NET 1.3.6.1.4.1.1166.1.200.2.36.0.128 Vendor Specific TLV (TLV-43) Start: VendorID 0803002040 Vendor Specific TLV (TLV-43) End: Num of TLV processed (in hex) 1D </pre>
Enterprise MIBs	
OID	Value
emtaInhibitSwDownloadDuringCall	false(2)
emtaFirewallEnable	true(1)
emtaRingWithDCOffset	false(2)
emtaIncludeInCmMaxCpe	false(2)
emtaDhcpOption	packetCableAndCableHomeObsolete(177)
emtaUseAlternateTelephonyRootCert	false(2)
emtaEnableDQoSLite	false(2)
emtaInhibitNcsSyslog	true(1)
emtaMaintenanceWindowBegin	Thu Jan 01 00:00:00 1970
emtaMaintenanceWindowDuration	0
emtaMaintenanceControlMask	0xmfrrb0 [maintenanceOnCmReset(0) maintenanceOnMtaReset(2) maintenanceOnCMSLoss(3)]
emtaMaintenanceQuarantineTimeout	120
emtaMaintenanceDisconnectedTimeout	120
emtaMaintenanceRFDisconnectTimeout	300
emtaSignalingAnnouncementCtrl	0x00
emtaSignalingVoiceJitterBufferType	jitterBufferTypeAdaptive(2)
emtaSignalingVoiceJitterNomValue	30
emtaSignalingVoiceJitterMinValue	0
emtaSignalingVoiceJitterMaxValue	60
emtaSignalingDataJitterNomValue	120
emtaSignalingDtmfToneRelayRFC2833Support	true(1)
emtaSignalingRtpBaseReceiveUdpPort	53456
emtaSignalingEndptConnectionCleanupTimeout	0
emtaSignalingEmaResetCleanupTimeout	0
emtaSignalingT38FaxRelaySupport	true(1)

Página del registro de eventos de MTA

Esta página muestra la información del registro de eventos de MTA y los mensajes de diagnóstico generados por MTA. Esta información está destinada a un técnico calificado.

Time	Priority	ID	Text
Endpoint			
2007-08-08 16:25:06	5-Information	35	MTA Last 24 Hours: Count of No ACK rec'd from Call Agent=0
mta001a66080b06.swdev.net/206.19.81.247			
2007-08-08 16:25:06	5-Information	35	MTA Last 24 Hours: Average Latency for Response to MGCP Messages=0 ms
mta001a66080b06.swdev.net/206.19.81.247			
2007-08-08 16:25:06	5-Information	35	MTA Last 24 Hours: Average Latency via RTCP Packets=0 ms
mta001a66080b06.swdev.net/206.19.81.247			
2007-08-08 16:25:06	5-Information	35	MTA Last 24 Hours: Maximum Jitter Measurements=0
mta001a66080b06.swdev.net/206.19.81.247			
2007-08-08 16:25:06	5-Information	35	MTA Last 24 Hours: Average Jitter Measurements=0
mta001a66080b06.swdev.net/206.19.81.247			
2007-08-07 16:25:06	5-Information	35	MTA Last 24 Hours: Count of No ACK rec'd from Call Agent=0

12

Solución de problemas

Si las soluciones presentadas aquí no resuelven el problema, comuníquese con su proveedor de servicio.

Antes de llamar a su proveedor de servicio, intente presionar el botón RESET (REINICIO) en el panel posterior de la unidad SVG1501.

Nota: Si presiona RESET (REINICIO), se restaurarán las configuraciones predeterminadas. Perderá los ajustes de configuración personalizados, incluidos Parental Control (Control para padres), Firewall y Advanced Settings (Configuraciones avanzadas).

El restablecimiento de la unidad SVG1501 puede demorar de cinco a 30 minutos. Su proveedor de servicios puede preguntarle el estado de los indicadores LED del panel frontal. Consulte [Indicadores LED del panel frontal y condiciones de error](#).

Soluciones

Tabla 1 – Solución de problemas

Problema	Posible solución
No se enciende la luz indicadora de alimentación.	<p>Verifique que la unidad SVG1501 esté correctamente enchufada al tomacorriente.</p> <p>Verifique que el tomacorriente funcione.</p> <p>Presione el botón RESET (REINICIO).</p>
No se pueden recibir ni enviar datos.	<p>Observe el estado de los indicadores LED en el panel frontal y consulte Indicadores LED del panel frontal y condiciones de error para identificar el error. Si tiene TV por cable, verifique que su TV esté funcionando y que la imagen se vea claramente. Si no puede sintonizar los canales de TV normales, el servicio de datos no funcionará.</p> <p>Verifique el cable coaxial en la unidad SVG1501 y el tomacorriente. Ajústelo manualmente si es necesario.</p> <p>Verifique la dirección IP. Siga los pasos para verificar la dirección IP para su sistema que se describe en Configuración de TCP/IP. Comuníquese con su proveedor de servicios si necesita una dirección IP.</p> <p>Verifique que el cable de Ethernet esté conectado correctamente a la unidad SVG1501 y al equipo.</p> <p>Verifique la conectividad de cualquier dispositivo conectado a través del puerto Ethernet, verificando los indicadores LED de conexión en el panel posterior.</p>

Problema	Posible solución
Los clientes inalámbricos no pueden enviar o recibir datos.	<p>Realice las primeras cuatro verificaciones en “Cannot send or receive data” (No se pueden recibir ni enviar datos).</p> <p>Verifique la configuración del modo de seguridad en la página de red principal inalámbrica:</p> <ul style="list-style-type: none"> • Si habilitó WPA y configuró una frase clave en la unidad SVG1501, asegúrese de que cada cliente inalámbrico afectado tenga la misma frase clave. Si esto no resuelve el problema, verifique que el cliente inalámbrico sea compatible con WPA. • Si habilitó WEP y configuró una clave en la unidad SVG1501, asegúrese de que cada cliente inalámbrico afectado tenga la misma clave WEP. Si esto no resuelve el problema, verifique que el adaptador inalámbrico del cliente sea compatible con el tipo de clave WEP configurado en la unidad SVG1501. • Para eliminar temporalmente el modo de seguridad como un problema potencia, deshabilite la seguridad. <p>Luego de resolver su problema, asegúrese de volver a habilitar la seguridad inalámbrica.</p> <ul style="list-style-type: none"> • En la página de control del acceso inalámbrico asegúrese de que la dirección MAC para cada cliente inalámbrico afectado esté correctamente detallada.
Baja velocidad de transmisión inalámbrica con WPA habilitado	<p>En la página de control del acceso inalámbrico verifique que el tipo de cifrado WPA sea TKIP. Si todos sus clientes inalámbricos son compatibles con AES, cambia el cifrado WPA a AES.</p>

Indicadores LED del panel frontal y condiciones de error

Los indicadores LED del panel frontal de la unidad SVG1501 brindan información de estado de las siguientes condiciones de error:

Tabla 2 – Indicadores LED del panel frontal y condiciones de error

LED	Estado	Si durante el arranque:	Si durante el funcionamiento normal:
POWER (ENCENDIDO)	APAGADO	La unidad SVG1501 no está enchufada correctamente al tomacorriente.	La unidad SVG1501 está desenchufada.
RECEIVE (RECIBIR)	DESTELLANDO	No se puede obtener el canal receptor.	Se perdió la conexión con el canal receptor.
SEND (ENVIAR)	DESTELLANDO	No se puede obtener el canal emisor.	Se perdió la conexión con el canal emisor.
ONLINE (EN LÍNEA)	DESTELLANDO	El registro de IP no se pudo completar.	Se perdió la conexión con el registro de IP.

A

Licencia de software

Puerta de enlace de voz inalámbrica SURFboard SVG1501

Motorola, Inc.

Home & Networks Mobility Solutions Business ("Motorola")

101 Tournament Drive

Horsham, PA 19044

IMPORTANTE: LEA ESTA LICENCIA DE SOFTWARE ("LICENCIA") CUIDADOSAMENTE ANTES DE INSTALAR, DESCARGAR O USAR CUALQUIER SOFTWARE DE APLICACIÓN, SOFTWARE DE CONTROLADOR DE USB, FIRMWARE Y DOCUMENTACIÓN RELACIONADA ("SOFTWARE") PROVISTA CON EL PRODUCTO DE DATOS POR CABLE ("PRODUCTO DE DATOS POR CABLE") DE MOTOROLA. EL USO DEL PRODUCTO DE DATOS POR CABLE Y/O LA INSTALACIÓN, DESCARGA O USO DE CUALQUIER SOFTWARE PROVISTO INDICA QUE USTED ACEPTA CADA UNA DE LAS CONDICIONES DE LA PRESENTE LICENCIA. DESDE SU ACEPTACIÓN, LA PRESENTE LICENCIA SERÁ UN CONTRATO LEGALMENTE VINCULANTE ENTRE USTED Y MOTOROLA. LAS CONDICIONES DE LA PRESENTE LICENCIA SE APLICAN A USTED Y CUALQUIER USUARIO FUTURO DE ESTE SOFTWARE.

SI USTED NO ESTÁ DE ACUERDO CON TODOS LOS TÉRMINOS DE LA PRESENTE LICENCIA (I) NO INSTALE NI USE EL SOFTWARE Y (II) DEVUELVA EL PRODUCTO DE DATOS POR CABLE Y EL SOFTWARE (COLECTIVAMENTE DENOMINADOS EL "PRODUCTO"), INCLUIDOS TODOS LOS COMPONENTES, DOCUMENTACIÓN Y TODOS LOS MATERIALES PROVISTOS CON EL PRODUCTO AL PUNTO DE COMPRA O A SU PROVEEDOR DE SERVICIO, SEGÚN CORRESPONDA, PARA RECIBIR UN REEMBOLSO TOTAL. AL INSTALAR O USAR EL SOFTWARE, USTED ESTÁ DE ACUERDO EN ACEPTAR LAS DISPOSICIONES DEL PRESENTE CONTRATO DE LICENCIA.

El Software incluye medios asociados, cualquier material impreso y toda documentación "en línea" o electrónica.

El Software provisto por terceros puede estar sujeto a contratos de licencia para usuario finales separados, emitidos por los fabricantes de dicho Software.

El Software nunca se vende. Motorola entrega el Software bajo licencia al cliente original y a todo licenciario posterior para uso personal solamente, sujeto a las condiciones de esta Licencia. Motorola y sus terceros licenciantes conservan los derechos de propiedad del Software.

Usted puede:

UTILIZAR este Software solamente en relación con el funcionamiento del Producto.

TRANSFERIR el Software a otra persona de forma permanente (junto con todas las piezas componentes y los materiales impresos), sólo si la persona acepta todas las condiciones de la presente Licencia. Si usted transfiere el Software, deberá al mismo tiempo transferir el Producto y todas las copias del Software (si corresponde) a la misma persona o destruir las copias no transferidas.

RESCINDIR la presente Licencia destruyendo el original y todas las copias del Software (si corresponde) realizadas por cualquier medio.

Usted no puede:

(1) dar en préstamo, distribuir, dar en alquiler o locación, transmitir, otorgar una sublicencia o transferir de algún otro modo el Software, en forma total o parcial, a persona alguna, con excepción de lo establecido en el párrafo TRANSFERIR precedente. (2) copiar o traducir la Guía del usuario que acompaña a este Software, excepto para uso personal. (3) copiar, modificar, traducir, descompilar, desarmar o alterar el diseño del Software, lo cual incluye pero no se limita a modificar el Software para que pueda operar en hardware no compatible. (4) quitar, alterar o impedir la visualización de las menciones de derecho de autor o los mensajes de inicio que se incluyen en el Software o en la documentación del Software. (5) exportar el Software o cualquiera de los componentes del Producto de forma que infrinja las normas de exportación de los Estados Unidos.

El Producto no ha sido diseñado ni está destinado para utilizar en el control de línea de aeronaves, tráfico aéreo, navegación de aeronaves comunicaciones de aeronaves; ni en el diseño, construcción, utilización o mantenimiento de instalaciones nucleares. MOTOROLA Y SUS TERCEROS LICENCIANTES NO OTORGAN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA DE APTITUD PARA DICHOS FINES. USTED MANIFIESTA Y GARANTIZA QUE NO USARÁ EL PRODUCTO PARA DICHOS FINES.

Motorola y sus terceros licenciantes conservarán en todo momento la titularidad de este Software y también la propiedad de los derechos de autor, los derechos sobre los trabajos de plantilla, patentes de invención, marcas comerciales y todos los demás derechos de propiedad intelectual que surjan de lo antedicho, y todas las adaptaciones y modificaciones a los derechos anteriormente mencionados. Motorola se reserva todos los derechos que no se otorgan bajo licencia expresamente en esta Licencia. El Software, incluidos cualquier imagen, gráfico, fotografía, animación, video, audio, música y texto incorporados a éste, es propiedad de Motorola o de sus terceros licenciantes y se encuentra protegido por las leyes sobre derechos de autor de los Estados Unidos y las disposiciones de los tratados internacionales. Salvo que se disponga expresamente lo contrario en la presente Licencia, la copia, reproducción, distribución o preparación de trabajos derivados del Software, de alguna parte del Producto o de la documentación, se encuentran terminantemente prohibidas por dichas leyes y tratados. Ninguna de las disposiciones de la presente Licencia se interpretará como una renuncia a los derechos de Motorola según las leyes sobre derechos de autor de los Estados Unidos.

La presente Licencia y todos los derechos del usuario que surgen de ella se rigen por las leyes de la Mancomunidad de Pensilvania, sin que sean de aplicación los principios que rigen los conflictos de leyes. LA PRESENTE LICENCIA SE CANCELARÁ AUTOMÁTICAMENTE en caso de que usted no cumpla con las condiciones de la presente Licencia.

Motorola no se hace responsable por el software de terceros suministrado como aplicación incluida o de cualquier forma junto con el Software.

DERECHOS RESTRINGIDOS DEL GOBIERNO DE LOS ESTADOS UNIDOS

El Producto y la documentación se suministran con DERECHOS RESTRINGIDOS. El uso, la reproducción o la divulgación del Gobierno están sujetos a las restricciones establecidas en la subdivisión (c)(1)(ii) de la cláusula Derechos sobre Datos Técnicos y Software de Computación (The Rights in Technical Data and Computer Software), bajo el número 52.227-7013. El contratista/fabricante es Motorola, Inc., Home & Networks Mobility Solutions Business, 101 Tournament Drive, Horsham, PA 19044.



Motorola, Inc.
101 Tournament Drive
Horsham, PA 19044 U.S.A.

<http://www.motorola.com>

MOTOROLA y el logotipo de la M estilizada están registrados en la Oficina de Patentes y Marcas Comerciales de los EE.UU. Todos los otros nombres de productos o servicios son propiedad de sus respectivos dueños. © 2009 Motorola, Inc.
Todos los derechos reservados.
567299-003-a
05/2009