

Manual de usuario

ASL-26555



Índice

ÍNDICE	2	EJEMPLO DEL ASL-26555 EN UNA RED 3G	19
ACERCA DE ESTE MANUAL DE USUARIO	5	CAPÍTULO 3: CONOCER EL ASL-26555	20
INTRODUCCIÓN	5	LOS LED	20
REQUISITOS DE SISTEMA	6	LOS PUERTOS.....	21
CARACTERÍSTICAS Y BENEFICIOS	7	LAS ANTENAS Y POSICIONES.....	22
INSTALACIÓN.....	8	CAPÍTULO 4: CONEXIÓN DEL ASL-26555	23
ANTES DE COMENZAR.....	8	DESCRIPCIÓN GENERAL	23
NOTAS ACERCA DE LA INSTALACIÓN.....	8	CONEXIONES.....	23
INFORMACIÓN QUE PRECISA DE SU PROVEEDOR DE SERVICIOS ADSL	10	CAPÍTULO 5: CONFIGURACIÓN DEL ASL-26555	26
INFORMACIÓN QUE VA A NECESITAR ACERCA DEL ASL-26555	11	DESCRIPCIÓN GENERAL	26
INFORMACIÓN QUE VA A NECESITAR ACERCA DE SU LAN U ORDENADOR.....	12	CAPÍTULO 6: MOVERSE POR LA PANTALLA DE CONFIGURACIÓN PRINCIPAL	28
INSTALACIÓN DEL DISPOSITIVO	13	CÓMO UTILIZAR LA UTILIDAD WEB	29
ALIMENTACIÓN DEL ROUTER	13	LA VENTANA DE SETUP (CONFIGURACIÓN) Y SUS SUBCARPETAS	29
BOTÓN DE RESTAURACIÓN A VALORES DE FÁBRICA	13	LA VENTANA DE ADVANCED (CONFIGURACIÓN AVANZADA) Y SUS SUBCARPETAS	32
CONEXIONES DE RED	14	LA VENTANA DE MAINTENANCE (MANTENIMIENTO) Y SUS SUBCARPETAS	37
COPYRIGHT Y MARCAS COMERCIALES REGISTRADAS	15	LA VENTANA DE STATUS (ESTADO) Y SUS SUBCARPETAS.....	39
CÓMO UTILIZAR ESTE MANUAL DE USUARIO.....	15	CAPÍTULO 7: CONFIGURACIÓN DEL ASL-26555 PARA INTERNET	41
CAPÍTULO 1	16	DESCRIPCIÓN GENERAL	41
BIENVENIDA	16	CAPÍTULO 8: CONFIGURACIÓN DEL ASL-26555 PARA LA CONECTIVIDAD INALÁMBRICA	44
CAPÍTULO 2: PLANIFICACIÓN DE SU RED	17	DESCRIPCIÓN GENERAL	44
TOPOLOGÍA DE RED	17	CAPÍTULO 9: CONFIGURACIÓN DEL ASL-26555 PARA LA CONECTIVIDAD 3G	48
DISPOSICIÓN DE LA RED	17		
ESTÁNDARES DE SEGURIDAD INALÁMBRICA	17		
EJEMPLO DEL ASL-26555 EN UNA RED TRADICIONAL.....	18		

OVERVIEW (DESCRIPCIÓN GENERAL)	48	DESCRIPCIÓN GENERAL	95
CAPÍTULO 10: CONFIGURACIÓN DE INTERNET	50	CAPÍTULO 20: CONFIGURACIÓN DE DNS Y DNS DINÁMICO	98
DESCRIPCIÓN GENERAL	50	DESCRIPCIÓN GENERAL	98
CAPÍTULO 11: CONFIGURACIÓN DE LA RED LOCAL	53	DNS DINÁMICO	99
DESCRIPCIÓN GENERAL	53	CAPÍTULO 21: TRABAJAR CON HERRAMIENTAS DE RED	104
CAPÍTULO 12: CONFIGURACIÓN DE LA HORA Y LA FECHA	58	DESCRIPCIÓN GENERAL	104
DESCRIPCIÓN GENERAL	58	MAPEO DE PUERTOS	105
CAPÍTULO 13: CONFIGURACIÓN DE LA CONEXIÓN INALÁMBRICA	60	ADDRMAP	106
DESCRIPCIÓN GENERAL	60	IGMP	107
CONFIGURACIÓN PROTEGIDA WI-FI	62	CALIDAD DE SERVICIO (QOS)	107
COMPRENDER LOS TIPOS DE WPA	68	UNIVERSAL PLUG N PLAY (UPNP)	113
ASPECTOS AVANZADOS DE LA CONFIGURACIÓN INALÁMBRICA	71	TR069	114
REGLAS DE ACCESO A LA WLAN	71	SAMBA	116
AÑADIR SSID MÚLTIPLES	72	SNMP	117
WLAN PERFORMANCE (RENDIMIENTO DE LA WLAN)	74	CAPÍTULO 22: CONFIGURACIÓN DEL ENRUTAMIENTO	120
CAPÍTULO 14: CONFIGURACIÓN DEL SERVIDOR VIRTUAL	76	DESCRIPCIÓN GENERAL	120
DESCRIPCIÓN GENERAL	76	CAPÍTULO 23: MANTENIMIENTO	124
CAPÍTULO 15: CONFIGURACIÓN DE APLICACIONES ESPECIALES	79	DESCRIPCIÓN GENERAL	124
DESCRIPCIÓN GENERAL	79	CAPÍTULO 24: TRABAJAR CON LA CONFIGURACIÓN DEL SISTEMA	127
CAPÍTULO 16: CONFIGURACIÓN DE LA DMZ	82	DESCRIPCIÓN GENERAL	127
DESCRIPCIÓN GENERAL	82	CAPÍTULO 25: TRABAJAR CON ACTUALIZACIONES DE FIRMWARE.	131
CAPÍTULO 17: CONFIGURACIÓN DEL CONTROL PARENTAL	85	DESCRIPCIÓN GENERAL	131
DESCRIPCIÓN GENERAL	85	CAPÍTULO 26: PRUEBA DE LOS AJUSTES	133
CONTROL PARENTAL – BLOQUEAR UN SITIO	87	DESCRIPCIÓN GENERAL	133
CONTROL PARENTAL – ELIMINACIÓN DE UN SITIO	88	CAPÍTULO 27: COMPRENDER EL REGISTRO DE SISTEMA	135
CAPÍTULO 18: CONFIGURACIÓN DE LA FUNCIÓN DE FILTRADO	90	DESCRIPCIÓN GENERAL	135
DESCRIPCIÓN GENERAL	90	CAPÍTULO 28: COMPRENDER LOS INFORMES DE ESTADO	137
CAPÍTULO 19: CONFIGURACIÓN DEL CORTAFUEGOS	95	DESCRIPCIÓN GENERAL	137
		INFORMACIÓN SOBRE EL DISPOSITIVO	137

INFORMACIÓN DE REGISTRO	140	DESCRIPCIÓN GENERAL	146
INFORMACIÓN USB	141	ESPECIFICACIONES TÉCNICAS	161
ESTADÍSTICAS	143		
CAPÍTULO 29: OBTENER AYUDA CON LA AYUDA	146		

Acerca de este Manual de usuario

Este Manual de usuario describe las funciones del ASL-26555. Está basado en la versión de firmware/software actual disponible para este producto y trata algunos de los nuevos e interesantes temas que nunca se han visto antes en esta línea de producto en una experiencia de lectura que merece la pena y que en última instancia sirve como guía para instalar y mantener el producto.

Introducción

CONEXIÓN A INTERNET ÓPTIMA

El ASL-26555 es un router versátil y de alto rendimiento tanto para el hogar como para oficinas pequeñas. Con ADSL2/2+ integrado y compatible con velocidades de bajada de hasta 24Mbps, protección mediante cortafuegos, calidad de servicio (QoS), LAN inalámbrica IEEE802.11n LAN y 4 puertos Ethernet, ofrece todas las funciones que precisa un hogar o una oficina pequeña para establecer una conexión segura y de alta velocidad con el mundo exterior.

CONEXIÓN INALÁMBRICA EXTREMA CON MÁXIMA SEGURIDAD

Este router ofrece velocidades inalámbricas hasta 4 veces por encima de las redes 802.11g. Puede maximizar el rendimiento inalámbrico conectando este router a ordenadores equipados con interfaces Gigabit y mantenerse conectado desde prácticamente cualquier punto de su hogar o su oficina. También puede emplearse con redes inalámbricas 802.11g y 802.11b para permitir una recepción mucho mejor. Es compatible con WPA-PSK y WEP para métodos de encriptación de datos y un acceso de usuario.

Movilidad 3G y conexión siempre activa

Con el ASL-26555 podrá conectar un módem 3G / HSDPA USB a su puerto USB integrado, lo que le permitirá utilizar una conexión a Internet 3G / HSDPA, UMTS, EDGE, GPRS o GSM, con velocidades de bajada de hasta 14.4 Mbps. Dada la creciente popularidad del estándar 3G, la comunicación a través del ASL-26555 resulta más cómoda y generalmente disponible, lo que le permitirá ver películas, descargarse música en movimiento o acceder a su correo electrónico desde cualquier lugar. Incluso podrá compartir su conexión a Internet con otras personas, independientemente de si está en una reunión o cruzando el país en tren. Su función de recuperación automática garantiza la máxima conectividad y unas interrupciones mínimas mediante una conexión rápida y sencilla a la red 3G en caso de producirse un fallo en su línea de ADSL. El ASL-26555 volverá a conectarse entonces automáticamente a la línea ADSL cuando se restaure la conexión, reduciendo así sus gastos. Estas funciones resultan perfectas para las oficinas, donde es imprescindible contar con conexión en todo momento.

Requisitos de sistema



Tenga en cuenta que éstos son los requisitos estrictamente mínimos necesarios para poder utilizar este router

1. Servicio a Internet ADSL suministrado por un proveedor de servicios de Internet (ISP).
2. Ordenador con procesador CPU a 200MHz o superior, 64MB o más de memoria RAM y unidad de CD-ROM.
3. Adaptador Ethernet con el protocolo TCP/IP instalado.
4. Navegador de Internet para la configuración (Internet Explorer v6 o superior, Firefox v1.5 o Safari 1.3 o superior)
5. Sistema operativo (Microsoft© Windows® XP/2000/Vista/Windows 7®)

Características y beneficios

- **Sencilla instalación** – El ASL-26555 utiliza cualquier navegador web estándar para configurar y gestionar cómodamente el router.
- **Compatibilidad DHCP** – El protocolo de configuración de host dinámico asigna de forma automática y dinámica todos los ajustes IP de la red LAN a cada host de su red. Con esto se elimina la necesidad de reconfigurar cada host siempre que se produce un cambio en la topología de la red. También es compatible con el enrutamiento de paquetes IP sobre WAN y bridges transparentes.
- **Traducción de direcciones de red (NAT)** – Para los entornos de pequeñas oficinas, el ASL-26555 permite a varios usuarios acceder al mismo tiempo a Internet a través de una sola cuenta. Esto permite a todos los que trabajan en la oficina acceder a Internet al precio de un solo usuario. De esta forma también se mejora la seguridad efectiva de la red al ocultar la red del hogar o SOHO tras una dirección IP global y visible. NAT ofrece mapeado de direcciones que puede emplearse también para vincular dos dominios IP a través de una conexión LAN a LAN.
- **Conectividad inalámbrica** – El ASL-26555 cumple con las normas IEEE 802.11a/b/g y, lo que es más importante, es compatible con la última IEEE 802.11n, lo que aumenta significativamente la tasa máxima de datos sin procesar de 54Mbit/s a 600Mbit/s.
- **Seguridad** – El ASL-26555 ofrece varias capas de seguridad, incluida la técnica de espectro ensanchado, control de direcciones MAC, identificación de dominios, encriptación y autenticación de usuarios.
- **Conformación del tráfico** – Se trata de un método para controlar la tasa de flujo de celdas de datos ATM. Esta función ayuda a establecer la calidad de servicio de la transferencia de datos ATM.
- **Alto rendimiento** – El ASL-26555 permite unas tasas de transferencia de datos muy altas de hasta 24 Mbps de velocidad de bajada utilizando el estándar ADSL 2+.
- **Gestión de red completa** – El router es compatible con SNMP (Protocolo Simple de Gestión de Redes) para una gestión web y una gestión de redes basada en texto a través de una conexión RS-232 o Telnet.
- **Conexión Telnet** – La conexión Telnet permite a un gestor de redes acceder al software de gestión del router a distancia.
- **Seguridad PPP (Protocolo Punto a Punto)**– El router es compatible con PAP (Protocolo de Autenticación de Contraseñas) y CHAP (Protocolo de Autenticación por Desafío Mutuo) para conexiones PPP. También es compatible con MSCHAP.

Instalación

Esta sección le llevará por el proceso de instalación. La ubicación del ASL-26555 es muy importante. No coloque el router en una zona cerrada como un armario, gabinete o en un ático o garaje.

Antes de comenzar

Lea y asegúrese de comprender todos los requisitos previos para la correcta instalación de su nuevo router. Deberá contar con toda la información y los equipos necesarios a mano antes de comenzar la instalación.

Notas acerca de la instalación

Para establecer una conexión con Internet, deberá dar información al router que se almacenará en su memoria. En el caso de algunos usuarios, sólo se necesitará su información de cuenta (nombre de usuario y contraseña). En el caso de otros, se precisarán varios parámetros que controlan y definen la conexión a Internet. Puede imprimir las dos páginas que siguen en las que se enumera esa información. De esta forma, contará con una copia en formato físico con toda la información necesaria para la configuración. Así, si tuviera que volver a configurar el dispositivo, podrá acceder fácilmente a toda la información necesaria. Asegúrese de mantener esta información de forma segura y privada.

Filtros de paso bajo

Puesto que los servicios ADSL y telefónico comparten los mismos cables de cobre para transportar sus respectivas señales, puede que se precise un mecanismo de filtrado para evitar las interferencias mutuas. Puede instalarse un dispositivo de paso bajo para cada teléfono que comparta la línea con la línea ADSL. Esos filtros son dispositivos pasivos fáciles de instalar que conectan el dispositivo ADLS y/o el teléfono utilizando el cable RJ-11 estándar. Pídale más información a su proveedor de servicios acerca del uso de filtros de paso bajo (también conocidos como microfiltros) en su instalación.

Sistemas operativos

El ASL-26555 utiliza un navegador para su configuración y gestión. Puede accederse al gestor de configuración web a través de cualquier sistema operativo capaz de ejecutar un programa navegador, incluidos Microsoft™ Windows® 98 SE, Windows® ME, Windows® 2000, Windows® XP, Windows® Vista y Windows® 7. El ASL-26555 también puede trabajar con otros sistemas operativos como MAC OSX y varias distribuciones Linux.

Navegador web

Puede utilizarse cualquier navegador web habitual para configurar el ASL-26555. El programa está diseñado para trabajar mejor con los últimos navegadores como Opera, Microsoft™ Internet Explorer® versión 6.0, Mozilla FireFox y Safari. El navegador web debe tener habilitado JavaScript. JavaScript está habilitado por defecto en muchos navegadores. Asegúrese de que JavaScript no ha sido deshabilitado por otros programas (como paquetes de seguridad de usuario web o de protección antivirus) que puedan estar ejecutándose en su ordenador.

Puerto Ethernet (adaptador NIC)

Cualquier ordenador que utilice el ASL-26555 debe ser capaz de conectarse con él a través del puerto Ethernet del router. Se trata de una conexión Ethernet y, por tanto, precisa que su ordenador esté equipado con un puerto Ethernet también. La mayoría de los ordenadores portátiles que se venden ahora ya tienen instalado un puerto Ethernet. De igual forma, la mayor parte de los ordenadores de sobremesa totalmente montados incluyen un adaptador NIC Ethernet de serie. Si su ordenador carece de puerto Ethernet, deberá instalar un adaptador NIC Ethernet para poder utilizar el ASL-26555. Si tiene que instalar el adaptador, siga las instrucciones de instalación que se incluyan con el mismo.

Software adicional

Puede que sea preciso instalar en su ordenador programas que le permitan acceder a Internet. Debe instalarse software adicional si va a utilizar el dispositivo como un simple bridge. Para una conexión en bridge, la información necesaria para realizar y mantener la conexión a Internet se almacena en otro ordenador o dispositivo de puerta de enlace, no en el propio router.

Si su servicio ADSL se suministra a través de una conexión PPPoE o PPPoA, la información necesaria para establecer y mantener la conexión a Internet puede almacenarse en el router. En ese caso, no será necesario instalar ningún programa en su ordenador. Sin embargo, puede que sea preciso modificar algunos ajustes en el dispositivo, incluida la información de cuenta necesaria para identificar y verificar la conexión.

Todas las conexiones a Internet precisan una dirección IP global única. En el caso de las conexiones en bridge, los ajustes IP globales deben residir en un dispositivo con el protocolo TCP/IP habilitado en el lado de la LAN del bridge, como un PC, un servidor, un dispositivo de puerta de enlace, un router o hardware cortafuegos similar. La dirección IP puede asignarse de varias formas. Su proveedor de servicios de Internet le dará instrucciones sobre cualquier programa de conexión o configuración NIC adicional que pueda ser preciso.

Información que precisa de su proveedor de servicios ADSL

Nombre de usuario

Se trata de su nombre de usuario para entrar en la red de su proveedor de servicios ADSL. Su proveedor de servicios ADSL lo emplea para identificar su cuenta.

Contraseña

Es la contraseña usada, junto con el nombre de usuario, para entrar en la red de su proveedor de servicios ADSL. Sirve para verificar la identidad de su cuenta.

Ajustes WAN / Tipo de conexión

Estos ajustes describen el método que emplea su proveedor de servicios ADSL para transportar datos entre Internet y su ordenador. La mayoría de los usuarios emplean la configuración por defecto. Puede que tenga que especificar una de las siguientes configuraciones de ajustes WAN y tipo de conexión (los ajustes de tipo de conexión se indican entre paréntesis):

- PPPoE/PPoA (PPPoE LLC, PPPoE VC-Mux, PPPoA LLC o PPPoA VC-Mux)
- Dirección IP dinámica o DHCP (1483 Bridged IP LLC o 1483 Bridged IP VC-Mux)
- Dirección IP estática (Bridged IP LLC, 1483 Bridged IP VC Mux, 1483 Routed IP LLC, 1483 Routed IP VC-Mux)
- Modo bridge (1483 Bridged IP LLC o 1483 Bridged IP VC Mux)

Tipo de modulación

El ADSL utiliza distintas técnicas de modulación estandarizadas para transmitir datos sobre las frecuencias de señal asignadas. Algunos usuarios pueden tener que cambiar el tipo de modulación empleada para su servicio. La modulación DSL por defecto (Autosense) empleada por el router detecta automáticamente todos los tipos de modulación ADSL, ADSL2 y ADSL2+.

Protocolo de seguridad

Se trata del método que empleará su proveedor de servicios ADSL para verificar su nombre de usuario y su contraseña cuando se registre en su red.

VPI

La mayoría de los usuarios no tendrán que modificar este ajuste. El Identificador de Ruta Virtual (VPI) se utiliza junto con el Identificador de Canal Virtual (VCI) para identificar la ruta de los datos entre la red de su proveedor de servicios ADSL y su ordenador. Si está configurando el router para varias conexiones virtuales, tendrá que configurar el VPI y el VCI de acuerdo con las instrucciones de su proveedor de servicios ADSL para cualquier conexión adicional. Esta configuración puede modificarse en la ventana de Configuración de la WAN de la interfaz de gestión web.

VCI

La mayoría de los usuarios no tendrán que modificar este ajuste. El Identificador de Canal Virtual (VCI) se utiliza junto con el Identificador de Ruta Virtual (VPI) para identificar la ruta de los datos entre la red de su proveedor de servicios ADSL y su ordenador. Si está configurando el router para varias conexiones virtuales, tendrá que configurar el VPI y el VCI de acuerdo con las instrucciones de su proveedor de servicios ADSL para cualquier conexión adicional. Esta configuración puede modificarse en la ventana de Configuración de la WAN de la interfaz de gestión web.

Información que va a necesitar acerca del ASL-26555

Nombre de usuario

Es el nombre de usuario necesario para acceder a la interfaz de gestión del router por defecto. Cuando trate de conectarse a través de un navegador web, se le pedirá que introduzca es nombre de usuario. El nombre de usuario por defecto es **1234**. El usuario no puede modificarlo.

Contraseña

Se trata de la contraseña que le pedirá que introduzca cuando acceda a la interfaz de gestión del router. La contraseña por defecto es **1234**. El usuario puede cambiarla.

Direcciones IP de la LAN para el ASL-26555

Se trata de la dirección IP que introducirá en el campo Dirección de su navegador web para acceder a la interfaz de usuario gráfica (GUI) del router. La dirección IP por defecto es 192.168.1.1. Puede modificarse para adaptarla a cualquier esquema de direcciones IP que desee el usuario. Esta dirección será la base de la dirección IP empleada para los servicios DHCP en la LAN cuando DHCP esté habilitado.

Máscara de subred LAN para el ASL-26555

Se trata de la máscara de subred empleada por el ASL-26555 y que se utilizará en toda su LAN. La máscara de subred por defecto es 255.255.255.0. Puede modificarse posteriormente.

Información que va a necesitar acerca de su LAN u ordenador

NIC Ethernet

Si su ordenador tiene una NIC Ethernet, puede conectar el ASL-26555 a ese puerto Ethernet empleando un cable Ethernet. También puede utilizar los puertos Ethernet en el ASL-26555 para conectarse con otros ordenadores o dispositivos Ethernet.

Estado de cliente DHCP

Su DSL- ASL-26555 está configurado por defecto para ser un servidor DHCP. Esto significa que puede asignar una dirección IP, máscara de subred y dirección de puerta de enlace por defecto a ordenadores dentro de su LAN. El rango de direcciones IP por defecto que asignará el ASL-26555 va de 192.168.1.2 a 192.168.1.254. Su ordenador o sus ordenadores deberán configurarse para obtener una dirección IP automáticamente (es decir, deberán configurarse como clientes DHCP).

Se recomienda que recopile y registre esa información aquí, o en algún otro lugar seguro, por si necesitara reconfigurar su conexión ADSL en el futuro. Cuando tenga esa información, estará listo para instalar y configurar su ASL-26555.

Instalación del dispositivo

El ASL-26555 conecta dos interfaces físicas separadas, una interfaz ADSL (WAN) y una interfaz Ethernet (LAN). Coloque el router en un lugar en el que pueda conectarse a los distintos dispositivos así como a una fuente de alimentación. El ASL-26555 no debería colocarse donde pueda estar expuesto a humedad o a un calor excesivo. Asegúrese de que los cables y el cable de alimentación están colocados de forma segura y no plantean ningún riesgo. Como cualquier dispositivo eléctrico, deberá observar los procedimientos de seguridad habituales.

El ASL-26555 puede colocarse sobre una estantería o escritorio, preferiblemente de forma que se puedan ver los indicadores LED de la parte frontal en caso de tener que resolver algún problema.

Alimentación del router

El ASL-26555 debe utilizarse con un transformador incluido con el aparato.

1. Introduzca el cable del transformador AC en el conector de alimentación que se encuentra situado en el panel posterior del router y conecte el transformador a una fuente de alimentación adecuada en las inmediaciones.
2. Pulse el botón de encendido. El indicador LED correspondiente debería encenderse y mantenerse encendido.
3. Si el puerto Ethernet está conectado a un dispositivo en uso, compruebe los indicadores LED Ethernet para asegurarse de que la conexión es válida. El router tratará de establecer la conexión ADSL, si la línea ADSL está conectada y el ASL-26555 está correctamente configurado, el LED se encenderá al cabo de unos segundos. Si es la primera vez que instala el dispositivo, puede que tenga que modificar algunos ajustes para que el ASL-26555 pueda establecer una conexión.

Botón de restauración a valores de fábrica

El ASL-26555 puede reiniciarse con su configuración original de fábrica con un clip. Apriete suavemente el botón de reinicio en la siguiente secuencia:

1. Asegúrese de que el ASL-26555 está encendido.
2. Mantenga pulsado el botón de reinicio de la parte trasera del dispositivo durante aproximadamente de 6 a 10 segundos.
3. Espere hasta que se reinicie el dispositivo.

Recuerde que esto borrará cualquier ajuste almacenado en la memoria flash, incluida la información de la cuenta de usuario y los ajustes IP de la LAN. La configuración del dispositivo volverá a la dirección IP por defecto de fábrica **192.168.1.1**, la máscara de subred será **255.255.255.0**, el nombre de usuario de gestión por defecto será **1234** y la contraseña por defecto será **1234**. También se definirá por defecto el usuario con el nombre de usuario **user** y la contraseña **user**.

Conexiones de red

Conexión de la red ADSL

Conecte un extremo del cable al puerto WLAN (RJ-11) en el panel trasero del ASL-26555 e introduzca el otro extremo en la toma mural RJ-11. Si está utilizando un dispositivo de filtro de paso bajo, siga las instrucciones incluidas con el dispositivo o que le haya suministrado su proveedor de servicios. La conexión a **Internet** representa la interfaz WAN, la conexión a Internet. Se trata de la conexión física con la infraestructura de red del proveedor y, en última instancia, con Internet.

Conexión del ASL-26555 a los puertos Ethernet

El ASL-26555 puede conectarse a un solo ordenador o dispositivo Ethernet a través del puerto Ethernet del panel posterior. Utilice cable de par trenzado estándar (CAT5 UTP) con conectores RJ-45. El puerto RJ-45 del router es un puerto cruzado (MDI-X). Siga las instrucciones Ethernet estándar al decidir qué tipo de cable va a emplear para realizar esa conexión. Al conectar el ASL-26555 directamente a un PC o servidor, utilice un cable de conexión directa normal. Debería emplear un cable cruzado al conectarlo a un puerto uplink (MDI-II) en un concentrador o conmutador. Las reglas que rigen la longitud del cable Ethernet se aplican también a la LAN y las conexiones del router. Asegúrese de que el cable que conecta la LAN con el router no supera los 100 metros.

Conexión concentrador o conmutador a router

Conecte el ASL-26555 a un puerto uplink (MDI-II) en un concentrador o conmutador Ethernet con un cable (CAT5 UTP). Si desea reservar el puerto uplink del conmutador o concentrador para otro dispositivo, conéctelo a cualquiera de los otros puertos MDI-X (1x, 2x, etc.) con un cable cruzado.

Conexión ordenador a router

Puede conectar el ASL-26555 directamente a una tarjeta de adaptador (NIC) Ethernet 10/100BASE-TX instalada en el PC con el cable Ethernet suministrado.

Copyright y marcas comerciales registradas

Las especificaciones están sujetas a cambios sin que medie notificación previa. Movistar es una marca comercial o una marca comercial registrada de Movistar y/o sus filiales en España y otros países. Copyright © 2010 Movistar. Reservados todos los derechos. Las otras marcas y denominaciones de producto son marcas comerciales o marcas comerciales registradas de sus respectivos titulares.

Cómo utilizar este Manual de usuario

El Manual de usuario del ASL-26555 se ha diseñado para facilitar más que nunca la comprensión de las redes ADSL inalámbricas además de la tecnología 3G. Preste atención a los siguientes elementos mientras esté leyendo el Manual.



Esta marca de verificación significa que se trata de una nota de interés y algo a lo que debería prestar especial atención al usar el dispositivo.



Esta exclamación significa que se trata de un aviso o advertencia y algo que podría dañar sus bienes o el dispositivo.



Esta interrogación señala un recordatorio sobre algo que podría tener que hacer al utilizar el dispositivo.

Capítulo 1

Bienvenida

Este Manual describe el router de Internet ASL-26555 con 3G. Este dispositivo es la solución perfecta para los usuarios domésticos y SOHO que precisan la última tecnología inalámbrica combinada con versatilidad para gestionar todas sus necesidades de redes

¿Cómo hace todo esto el dispositivo? El ASL-26555 ofrece el máximo alcance y versatilidad dentro de su red inalámbrica permitiéndole al mismo tiempo conectar la red inalámbrica a un entorno cableado. De hecho, el ASL-26555 admite las comunicaciones en hasta cuatro dispositivos de red cableados en un área y varias conexiones inalámbricas.

El ASL-26555 ofrece la comodidad de la capacidad 3G, por lo que puede conectarse a través de la red 3G si la conexión ADSL se ve interrumpida. Todo lo que necesita es un adaptador USB 3G separado para introducirlo en el puerto USB. Las velocidades de conexión van de 3.5Mbit/s a 7Mbit/s y el módem 3G puede admitir a cualquiera en la red.

Pero, ¿qué significa todo esto?

Las redes son herramientas muy útiles para compartir recursos informáticos. Permiten acceder a una impresora desde distintos ordenadores y acceder a datos almacenados en el disco duro de otro equipo. Las redes se utilizan incluso para jugar a videojuegos multijugador. De esta forma, las redes son útiles no sólo en los hogares y oficinas, sino que también pueden resultar divertidas. Los PC de una red cableada pueden crear una LAN, o red de área local. Se conectan a través de cables Ethernet, y por eso la red se denomina "cableada". Al compartir la misma configuración, dentro de su radio de transmisión, también pueden transmitir datos de forma inalámbrica. De esta forma se reduce la necesidad de utilizar cables Ethernet y la gestión centralizada concede a los administradores del sistema un control completo.

Utilice las instrucciones de este Manual como ayuda para conectar el router con 3G, configurarlo para que actúe como bridge de sus distintas redes. Estas instrucciones deberían ser todo lo que necesite para aprovechar al máximo su ASL-26555.

Capítulo 2: Planificación de su red

Topología de red

El router ASL-26555 cumple los estándares ADSL mundiales, admite velocidades de bajada de hasta 12/24 Mbps con ADSL 2/2, 8 Mbps con ADSL, y velocidades de subida de hasta 1 Mbps. Los usuarios podrán disfrutar no sólo de conexiones ADSL2+ de alta velocidad, sino también ejecutar aplicaciones de banda ancha como juegos interactivos, streaming de vídeo y servicios VOIP mucho más fácilmente que antes. El ASL-26555 puede conectarse a impresoras, unidades externas e incluso NAS.

La interfaz de usuario web hace el ASL-26555 extremadamente sencillo de instalar y facilita enormemente la gestión de la red a los usuarios. El router es compatible con DHCP, lo que significa que las direcciones IP pueden configurarse y asignarse automáticamente a los equipos cliente. La seguridad inalámbrica también se ha mejorado a través de la autenticación SSID. Además de admitir 802.11n, presenta compatibilidad con equipos 802.11g y 802.11b ya existentes. Las funciones inalámbricas de acceso protegido (WPA-PSK/WPA2-PSK) y privacidad equivalente cableada (WEP) mejoran el nivel de protección de los datos y control del acceso a través de una LAN inalámbrica.

Disposición de la red

El ASL-26555 se ha diseñado para ser utilizado con productos similares dentro de su rango. El router principal es compatible con todos los dispositivos Movistar dentro de la misma disposición de red y funciona sin problemas en todos los espectros. El ASL-26555 funciona en un entorno LAN de banda ancha, una disposición de infraestructura inalámbrica y ofrece compatibilidad de conexión 3G para otros dispositivos asociados al router.

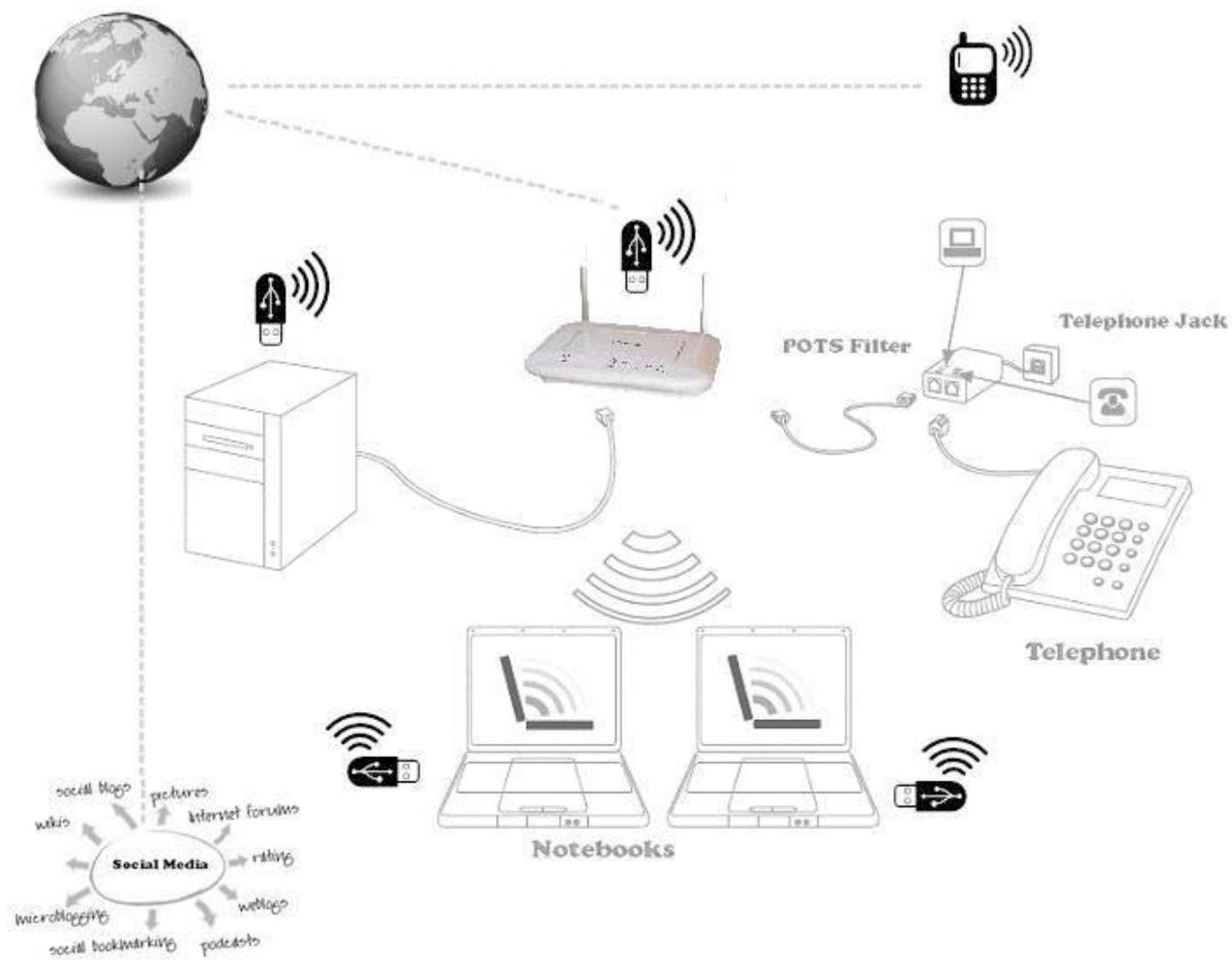
Estándares de seguridad inalámbrica

El primer y más importante estándar de seguridad que se creó fue el WEP (privacidad equivalente inalámbrica). Pretendía dotar de seguridad a las conexiones inalámbricas y empleaba una longitud de clave media de 128-256-bits. Sin embargo, este estándar pronto resultó inservible ya que los hackers encontraron formas de piratear las claves. Se publicó un estándar mejorado para superar esas vulnerabilidades denominado WPA (acceso protegido wi-fi). WPA es una mejora de software/firmware con respecto a WEP ya que resulta más difícil de piratear. WPA utiliza una clave pre-compartida (PSK) para establecer la seguridad empleando una paráfrasis de 8 a 63 caracteres o una cadena hexadecimal de 64 caracteres. Es más difícil que un hacker pueda piratear esta clave de seguridad y por tanto se recomienda por defecto en el ASL-26555. Con los años, se han registrado avances que mejoran la seguridad del estándar WPA y lo protegen de los piratas. El último estándar 802.11i es un paquete de seguridad riguroso que utilice el último hardware/firmware. Ha sido bautizado por la WiFi Alliance como WPA2. La solidez de WPA y WPA2 reside en que ambos son compatibles con métodos de autenticación EAP con servidores RADIUS y claves precompartidas (PSK). Esto permite una mejor autenticación. La mayoría de los dispositivos comerciales se han pasado de WEP a WPA2 ya que WEP ha resultado demasiado poco seguro. WPA2 es más seguro que WPA. Sin embargo, carecer de seguridad deja su sistema y su red muy vulnerables. Le recomendamos que aplique algún tipo de seguridad en su sistema.

Ejemplo del ASL-26555 en una red tradicional



Ejemplo del ASL-26555 en una red 3G



La línea discontinua indica una conexión a **Internet**.



Esta imagen indica un módem 3G conectado a la red

Capítulo 3: Conocer el ASL-26555

Los LED

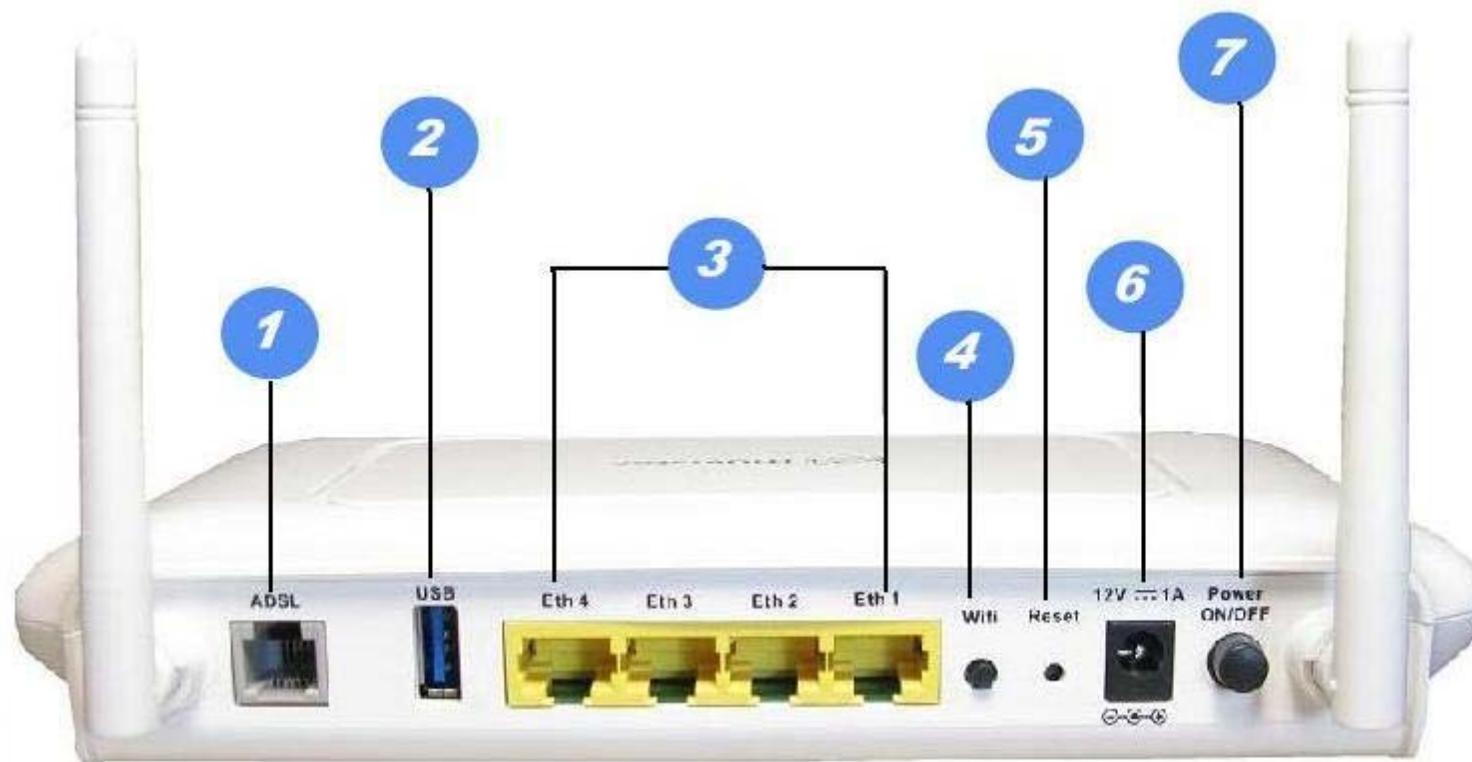
Los LED de los puntos de acceso, donde se visualiza información sobre la actividad de la red, se encuentran en el panel frontal.



1	Encendido:	LED verde fijo que indica que la unidad está encendida.
2	Ethernet	LED que parpadea en verde indicando actividad en la red.
3	Wifi	LED que parpadea en verde indicando actividad inalámbrica.
4	3G:	LED que parpadea en verde cuando en adaptador USB 3G está activo y funcionando.
5	ADSL:	LED que parpadea en verde cuando la línea ADSL se ha sincronizado correctamente.
6	Internet:	LED que parpadea en verde cuando el dispositivo se ha autenticado con el ISP.

Los puertos

Los puertos de los puntos de acceso se encuentran en la parte trasera del dispositivo.



1	Puerto ADSL:	Se trata de un puerto de línea RJ-11 ADSL que conecta el router con la línea ADSL.
2	Puertos USB:	El puerto USB está destinado a los dispositivos de almacenamiento, impresoras y adaptador USB 3G.
3	Puertos LAN (1-4):	Se trata de puertos LAN Fast Ethernet que conectan este router con la red local utilizando cables CAT5.
4	Botón WiFi:	Pulse este botón para encender o apagar la LAN inalámbrica.
5	Botón de reinicio:	Mantenga pulsado este botón durante 6 segundos para reiniciar el dispositivo con los valores por defecto.
6	Conector de alimentación:	El transformador suministrado se conecta aquí.
7	Botón de encendido:	Pulse este botón para encender y apagar el dispositivo.



Puerto: El punto de conexión en un ordenador o dispositivo de red utilizada para conectar cables o transformadores.



IMPORTANTE: Si reinicia el router con sus parámetros por defecto borrará toda su configuración (incluidos los ajustes de seguridad inalámbrica, direcciones IP y SSID) y la sustituirá por los valores de fábrica. No reinicie el router si quiere conservar su configuración.

Las antenas y posiciones

Las antenas del punto de acceso se encuentran en la parte trasera del dispositivo. El punto de acceso puede colocarse sobre un escritorio o montarse en una pared. Si se coloca sobre un escritorio, no puede apilarse. El punto de acceso cuenta con dos antenas omnidireccionales de 2dBi no desmontables. Ajústelas de manera que formen un ángulo de 90 grados para obtener el máximo rendimiento.



Capítulo 4: Conexión del ASL-26555

Descripción general

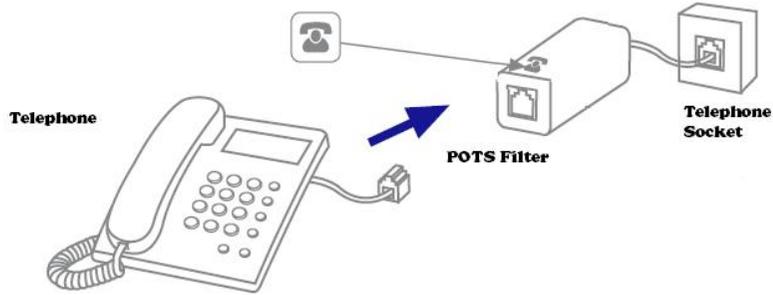
Este capítulo explica cómo colocar y conectar el punto de acceso.

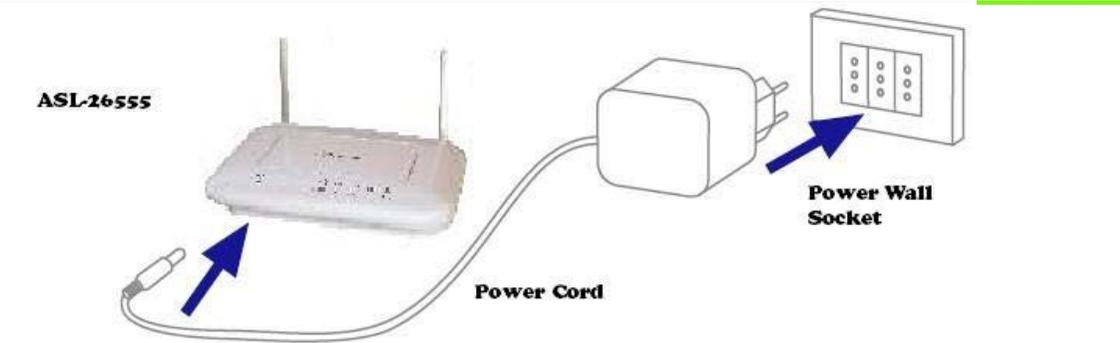
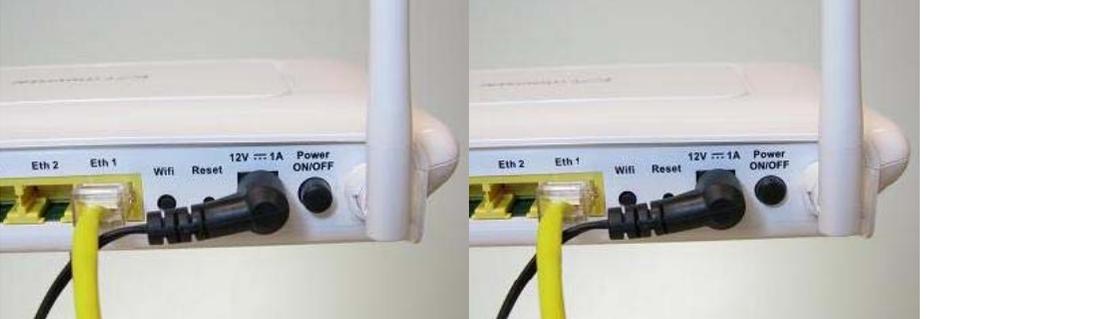


En función de su aplicación, puede que quiera configurar el dispositivo antes de encenderlo. Consulte **Instalación del dispositivo**.

Conexiones

<p>Paso 1:</p>	<p>Desconecte el teléfono y la línea telefónica (cable RJ-11) de la toma mural.</p>	<p>Telephone</p> <p>Telephone Socket</p>
<p>Paso 2:</p>	<p>Conecte la línea telefónica del microfiltro compuesto (cable RJ-11) a la toma de teléfono. Conecte un extremo del cable telefónico (cable RJ-11) incluido en la caja, a la toma del microfiltro señalada con el icono de un router. En la toma del microfiltro señalada con el icono de un teléfono, puede conectar un aparato telefónico.</p>	<p>POTS Filter</p> <p>Router</p> <p>Telephone socket</p>

<p>Paso 3:</p>	<p>Conecte el otro extremo del cable telefónico (cable RJ-11) al puerto ADSL de la parte posterior del ASL-26555.</p>	
<p>Paso 4:</p>	<p>Puede conectar otros aparatos telefónicos en otras tomas de teléfono. Para ello, conecte un microfiltro simple a la toma de teléfono y un aparato telefónico al conector señalado con el icono de un teléfono del microfiltro simple.</p>	
<p>Paso 5:</p>	<p>Conecte un extremo del cable Ethernet (RJ-45) a un puerto abierto en la parte posterior del ASL-26555. Conecte el otro extremo del cable Ethernet a un PC.</p>	
<p>Paso 6:</p>	<p>Conecte el cable de alimentación en la parte posterior del ASL-26555.</p>	

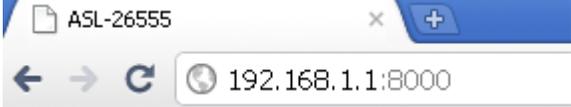
<p>Paso 7: Conecte la clavija en la toma mural.</p>	 <p>The diagram illustrates the power connection for the ASL-26555 router. A power cord is shown with one end connected to the router's power jack and the other end plugged into a standard wall socket. Labels with arrows point to the router (ASL-26555), the power cord (Power Cord), and the wall socket (Power Wall Socket).</p>
<p>Paso 8: Pulse el botón "Power ON/OFF" para encender el ASL-26555.</p>	 <p>Two side-by-side photographs of the ASL-26555 router's rear panel. The left photo shows the power jack with a power cord plugged in. The right photo shows the Power ON/OFF button. Labels on the panel include Eth 2, Eth 1, Wifi, Reset, 12V --- 1A, and Power ON/OFF.</p>

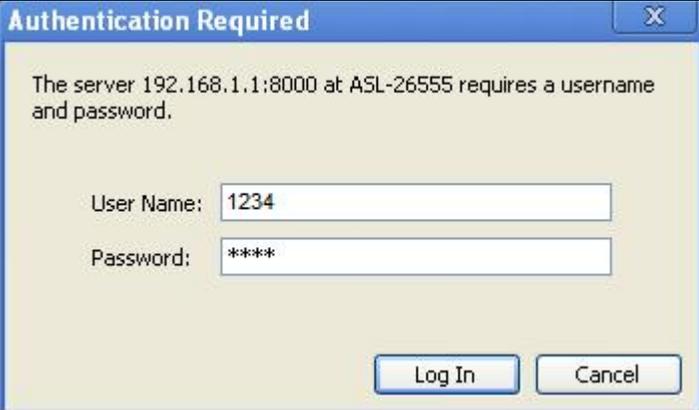
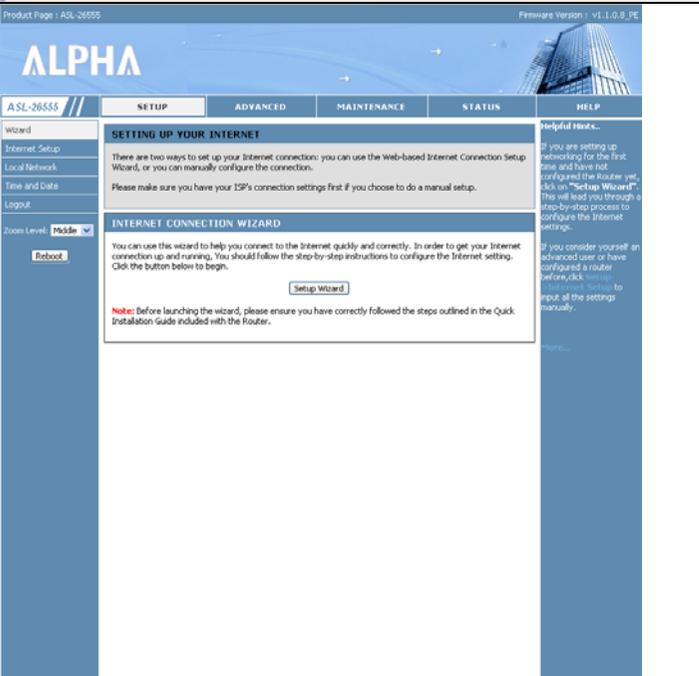
Capítulo 5: Configuración del ASL-26555

Descripción general

El punto de acceso se ha diseñado para que resulte funcional desde el momento en que se saca de la caja utilizando la configuración por defecto. Sin embargo, si desea modificar esos ajustes, puede configurar el punto de acceso a través de un navegador web con su utilidad web. Este capítulo explica como utilizar esa utilidad para realizar los principales ajustes básicos.

Puede acceder a la utilidad a través de navegadores web como Microsoft Internet Explorer, Mozilla Firefox, Safari u Opera empleando un ordenador que esté conectado al punto de acceso.

Paso 1:	Haga doble clic en su navegador favorito.	
Paso 2:	Escriba el puerto y la dirección IP por defecto en la barra de navegación del ASL-26555.  La dirección IP por defecto es: 192.168.1.1:8000	

<p>Paso 3:</p>	<p>Escriba un User Name (nombre de usuario) y una Password (contraseña) y haga clic en Log In</p> <p> <ul style="list-style-type: none"> • El Nombre de usuario por defecto es: 1234 • La contraseña por defecto es: 1234 </p>	 <p>The server 192.168.1.1:8000 at ASL-26555 requires a username and password.</p> <p>User Name: <input type="text" value="1234"/></p> <p>Password: <input type="password" value="****"/></p> <p>Log In Cancel</p>	
<p>Paso 4:</p>	<p>Aparecerá la ventana de configuración principal.</p>	 <p>Product Page / ASL-26555 Firmware Version: V1.1.0.8_1E</p> <p>ALPHA</p> <p>ASL-26555 // SETUP ADVANCED MAINTENANCE STATUS HELP</p> <p>Wizard</p> <p>Internet Setup: There are two ways to set up your Internet connection: you can use the Web-based Internet Connection Setup Wizard, or you can manually configure the connection.</p> <p>Local Network</p> <p>Time and Date: Please make sure you have your ISP's connection settings first if you choose to do a manual setup.</p> <p>Logout</p> <p>Zoom Level: 100%</p> <p>Internet Connection Wizard</p> <p>You can use this wizard to help you connect to the Internet quickly and correctly. In order to get your Internet connection up and running, you should follow the step-by-step instructions to configure the Internet setting. Click the button below to begin.</p> <p>Setup Wizard</p> <p>Note: Before launching the wizard, please ensure you have correctly followed the steps outlined in the Quick Installation Guide included with the Router.</p> <p>Helpful hints... If you are setting up networking for the first time and have not configured the Router, you click on "Setup Wizard". This will lead you through a step-by-step process to configure the Internet settings. If you consider yourself an advanced user or have configured a router before, click "Manual Setup" to input all the settings manually.</p>	
<p>Paso 5:</p>	<p>Haga clic en Setup Wizard para comenzar la configuración.</p>		

Capítulo 6: Moverse por la pantalla de configuración principal

Moverse por la pantalla de configuración principal es fácil y sencillo. Está dividida en dos ventanas. La barra de navegación, **1-5**, contiene las principales ventanas de configuración para las distintas funciones. La barra de herramientas de la izquierda, **6**, contiene secciones separadas para cada ventana de configuración principal individual. El cuerpo, **7**, es la zona de configuración principal, y la barra de herramientas de la derecha, **8**, contiene consejos útiles para cada secuencia de configuración. Cada ventana de configuración contiene una explicación detallada de las modificaciones e los ajustes.

Product Page : ASL-26555 Firmware Version : v1.1.0.8_PE

ALPHA

ASL-26555 // **1** SETUP **2** ADVANCED **3** MAINTENANCE **4** STATUS **5** HELP

Wizard
Internet Setup
Local Network
Time and Date
Logout
Zoom Level: Middle
Reboot **6**

SETTING UP YOUR INTERNET

There are two ways to set up your Internet connection: you can use the Web-based Internet Connection Setup Wizard, or you can manually configure the connection.

Please make sure you have your ISP's connection settings first if you choose to do a manual setup.

INTERNET CONNECTION WIZARD

You can use this wizard to help you connect to the Internet quickly and correctly. In order to get your Internet connection up and running, You should follow the step-by-step instructions to configure the Internet setting. Click the button below to begin.

7 Setup Wizard

Note: Before launching the wizard, please ensure you have correctly followed the steps outlined in the Quick Installation Guide included with the Router.

Helpful Hints..
If you are setting up networking for the first time and have not configured the Router yet, click on "Setup Wizard". This will lead you through a step-by-step process to configure the Internet settings.
If you consider yourself an advanced user or have configured a router before, click Setup->Internet Setup to input all the settings manually. **8**
More...

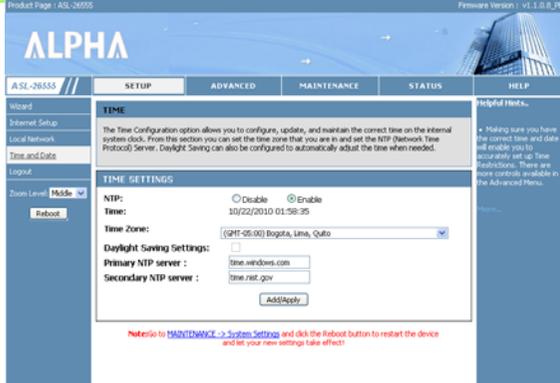
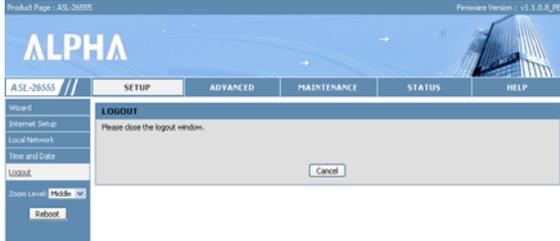
Cómo utilizar la utilidad web

La ventana de SETUP (Configuración) y sus subcarpetas

Para comprender y apreciar plenamente la conveniencia de la utilidad web, a continuación encontrará una breve explicación. La utilidad web es una herramienta muy potente que debe ser utilizada por los administradores de sistemas. Si no es usted un administrador, consulte a un profesional. Vamos a echar un vistazo a la barra de herramientas de navegación (6) de la parte izquierda de la pantalla principal. Cada sección tiene su propia ventana principal y se configura por separado. Sigue una visión más de cerca de lo que son y lo que significan:

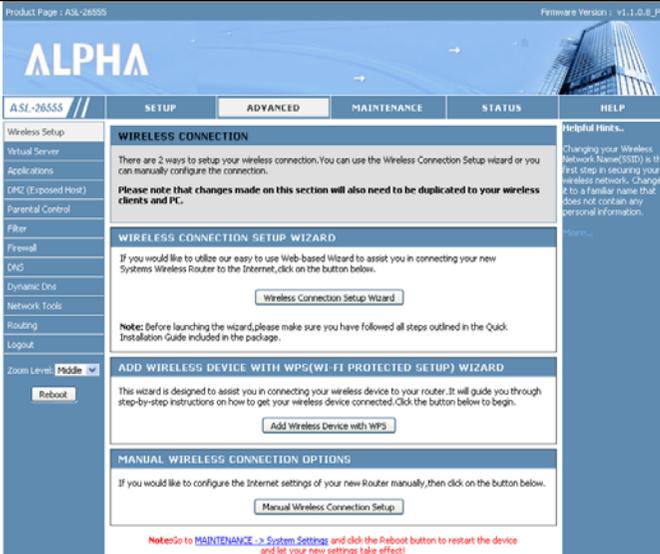
<p>1</p>	<p>Wizard: Esta ventana muestra un asistente fácil de utilizar para la configuración de Internet y la conectividad inalámbrica.</p>	
<p>2</p>	<p>Internet Setup: Esta ventana permite la configuración manual del ADSL y 3G.</p>	

<p>3</p>	<p>Local Network (Red local): Esta primera captura de pantalla se ocupa de la configuración del router y el mapeo de puertos.</p>	
	<p>Local Network: La segunda ventana permite a los usuarios configurar manualmente los ajustes de Red local y DHCP.</p>	
	<p>Local Network: La tercera ventana permite a los usuarios configurar direcciones IP estáticas, listas de reserva DHCP y listas de clientes DHCP.</p>	

<p>4</p>	<p>Time and Date (Fecha y hora): Aquí, los usuarios pueden configurar la zona horaria del ASL-26555 y sincronizarse con los servidores de hora.</p>	
<p>5</p>	<p>Logout: Esta pantalla saca al usuario del ASL-26555 y le pide que cierre el navegador.</p>	

La barra de navegación superior ofrece ajustes avanzados para el ASL-26555. Si hace clic en cada sección de la barra de navegación aparecerán ajustes más detallados en la barra de herramientas de la izquierda. Encontrará una descripción más pormenorizada de cada sección en los capítulos que siguen.

La ventana de ADVANCED (Configuración avanzada) y sus subcarpetas

<p>1</p>	<p>Wireless Setup (Asistente de configuración): Esta ventana se divide en tres partes: 1) el Asistente de configuración inalámbrica, 2) el Asistente de configuración protegida WI-FI, y 3) la Configuración de conexión inalámbrica manual.</p>	
<p>2</p>	<p>Virtual Server: El ASL-26555 actúa y puede configurarse como un servidor virtual.</p>	

3

Applications : Configure los puertos de apertura/cierre para permitir que las aplicaciones sorteen el cortafuegos.

SPECIAL APPLICATION

The Application is used to open single or multiple ports in your firewall when the router sends data out to the Internet on a outgoing "Trigger" port or port range. Applications that apply to all computers on your internal network.

SPECIAL APPLICATION

Enable Application: Disabled Enabled

Name:

Trigger Port Start:

Trigger Port End:

Trigger Traffic Protocol Type:

Trigger Source IP:

Open Port:

Open Traffic Protocol Type:

EXISTING APPLICATION

Status	Name	Trigger Source IP/port	Trigger Traffic Protocol Type	Open Ports	Open Traffic Protocol Type	Remove	Edit
Inactive	Barfe.net	Any/8112	All Protocol	4112	All Protocol	<input type="checkbox"/>	<input type="checkbox"/>
Inactive	Chidex	Any/727*	All Protocol	51200-51281, 12310	All Protocol	<input type="checkbox"/>	<input type="checkbox"/>
Inactive	ECU II	Any/2019*	All Protocol	2000-2030, 2030-2030, 2030-2030, 2030-2030, 600	All Protocol	<input type="checkbox"/>	<input type="checkbox"/>
Inactive	MSN Gaming Zone	Any/4724*	All Protocol	2200-2400, 2800-3000	All Protocol	<input type="checkbox"/>	<input type="checkbox"/>
Inactive	PC via Phone	Any/2053*	All Protocol	51210, 52122	All Protocol	<input type="checkbox"/>	<input type="checkbox"/>
Inactive	Quick Time 4	Any/854*	All Protocol	6876-6999	All Protocol	<input type="checkbox"/>	<input type="checkbox"/>
Active	XBOX360-1	Any/2074*	All Protocol	3074	All Protocol	<input type="checkbox"/>	<input type="checkbox"/>
Active	XBOX360-2	Any/88*	UDP	88	UDP	<input type="checkbox"/>	<input type="checkbox"/>

Note: Go to [MAINTENANCE](#) > [System Settings](#) and click the [Reboot](#) button to restart the device and let your new settings take effect!

4

DMZ (Exposed Host): Permite acceder a PC cliente a la misma red.

DMZ (EXPOSED HOST)

DMZ (Exposed Host): From the Internet you can access to a client within the DMZ. This client is more vulnerable than the other clients in your LAN. It is strongly recommended to store any sensitive data behind the DMZ protected by a firewall.

Note: Most of packets that from Internet will be forwarding to DMZ server except those packets that should forward to active virtual server, or access SAC's Telnet/FTP/joomla administration key access service.

DMZ (EXPOSED HOST) SETTINGS

Enable DMZ: Disable Enable

IP Address:

Time:

Begin time:

End time:

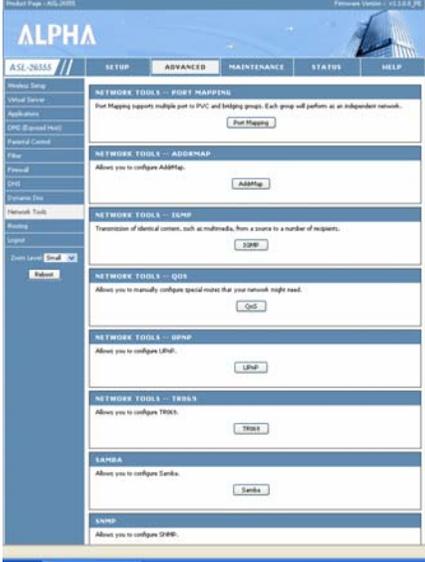
Begin day:

End day:

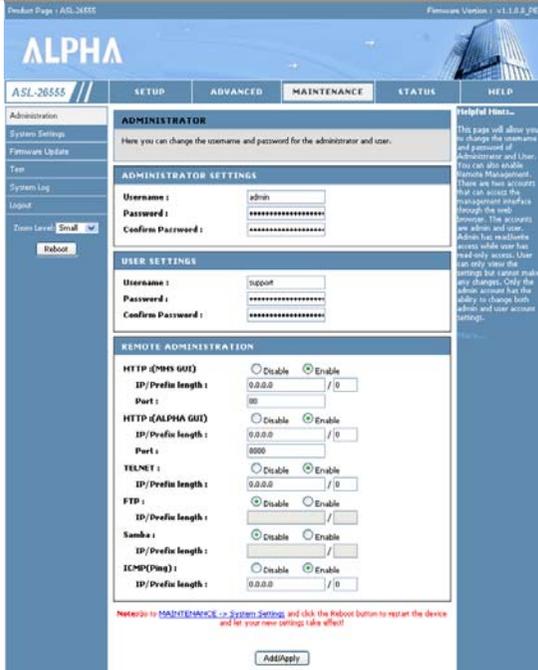
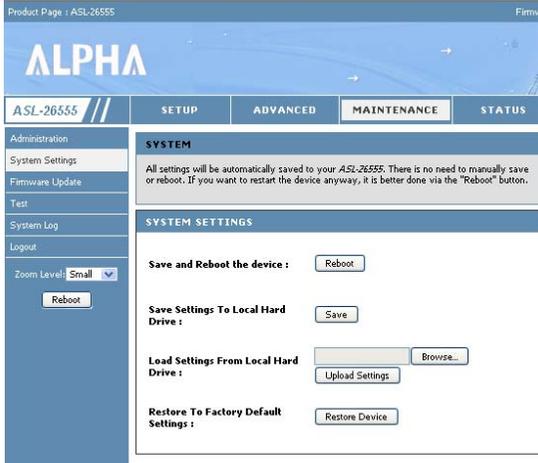
Note: Go to [MAINTENANCE](#) > [System Settings](#) and click the [Reboot](#) button to restart the device and let your new settings take effect!

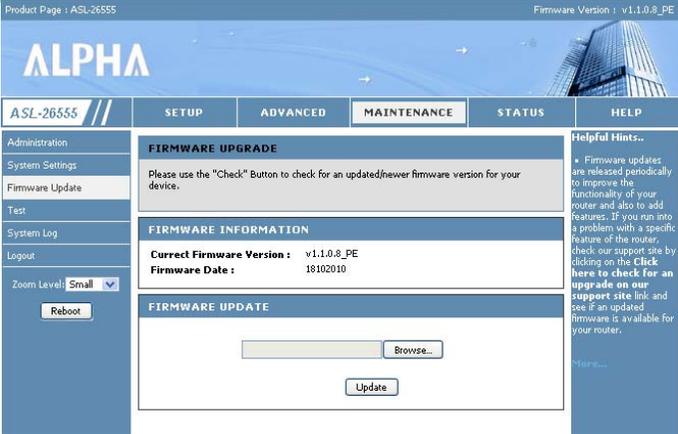
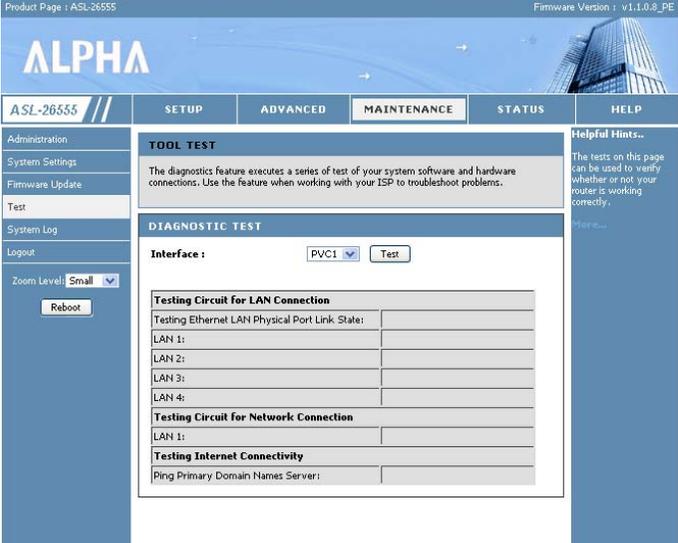
<p>5</p>	<p>Parental Control (Control parental): Configure lo que quiere permitir y no permitir que vean sus hijos.</p>	
<p>6</p>	<p>Filter (Filtro): Los filtros gestionan el acceso de los usuarios de la LAN a Internet</p>	

<p>7</p>	<p>Firewall (Cortafuegos): Los cortafuegos permiten o deniegan el paso del tráfico a través del dispositivo.</p>	
<p>8</p>	<p>DNS: El servidor DNS traduce un nombre de domino (URL) en una dirección IP.</p>	
<p>9</p>	<p>Dynamic DNS (DNS dinámico): Define los ajustes DNS.</p>	

<p>10</p>	<p>Network Tools (Herramientas de red): Distintas herramientas para diagnosticar paquetes.</p>	
<p>11</p>	<p>Routing (Enrutamiento): Configure o edite la tabla de enrutamiento.</p>	

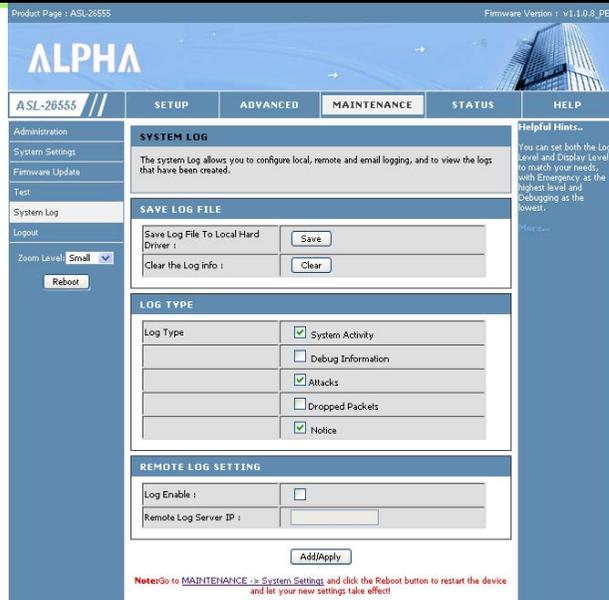
La ventana de MAINTENANCE (Mantenimiento) y sus subcarpetas

<p>1</p>	<p>Administration (Administración): Todos los ajustes y funciones de administración básicas pueden editarse aquí.</p>	 <p>The screenshot shows the ALPHA web interface with the 'MAINTENANCE' tab selected. The left sidebar contains a menu with 'Administration' highlighted. The main content area is divided into three sections: 'ADMINISTRATOR' (with fields for Username and Password), 'USER SETTINGS' (with fields for Username and Password), and 'REMOTE ADMINISTRATION' (with sections for HTTP (HMS GUI), HTTP (ALPHA GUI), TELNET, FTP, Samba, and ICMP(Ping), each with 'Disable' and 'Enable' radio buttons and IP/Prefix length fields). A 'Reboot' button is visible at the bottom of the main content area.</p>
<p>2</p>	<p>System Settings (Configuración de sistema): Información sobre la configuración del sistema.</p>	 <p>The screenshot shows the ALPHA web interface with the 'MAINTENANCE' tab selected and the 'SYSTEM' sub-tab active. The left sidebar contains a menu with 'System Settings' highlighted. The main content area is titled 'SYSTEM' and contains 'SYSTEM SETTINGS' with buttons for 'Reboot', 'Save', 'Browse...', 'Upload Settings', and 'Restore Device'. A 'Reboot' button is also present in the sidebar.</p>

<p>3</p>	<p>Firmware Update (Actualización de firmware): Detalles sobre la versión de firmware y los procedimientos de actualización.</p>	
<p>4</p>	<p>Test: Prueba de los fallos del sistema.</p>	

5

System Log (Registro del sistema): El sistema le permite configurar registros locales, remotos o por e-mail y ver los registros creados.

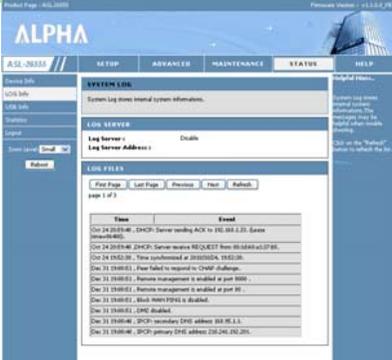
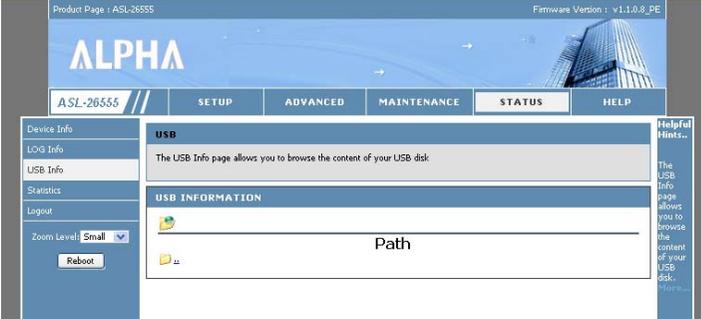
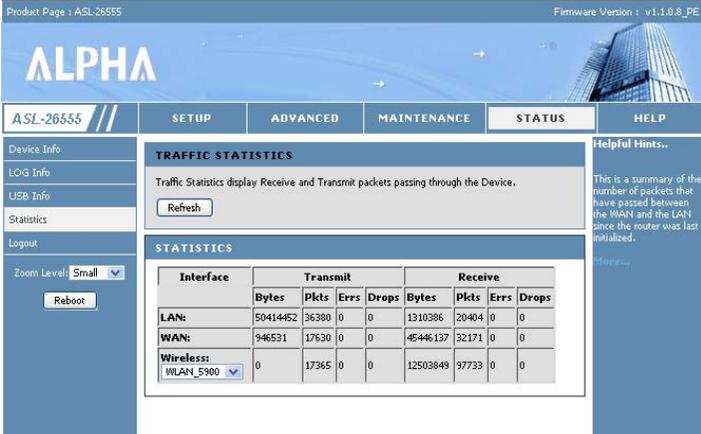


La ventana de STATUS (Estado) y sus subcarpetas

1

Device Info (Información del dispositivo): Le permite comprobar el estado de las redes de Internet, inalámbricas y LAN.

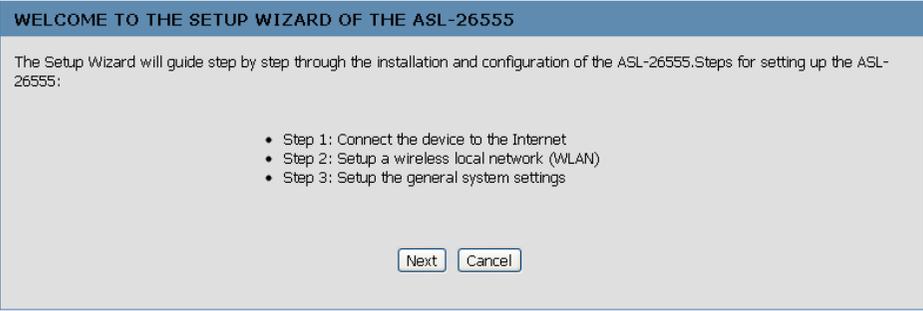


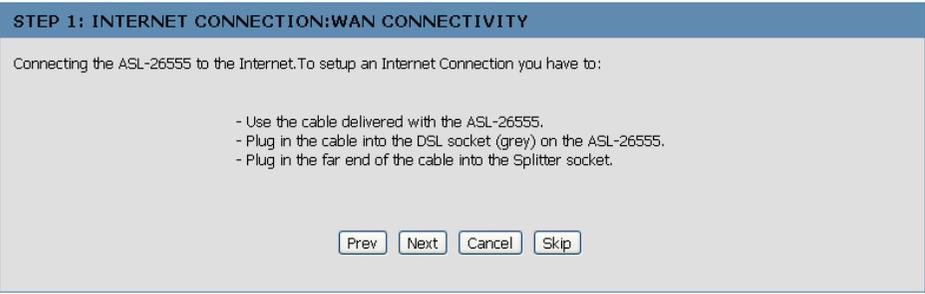
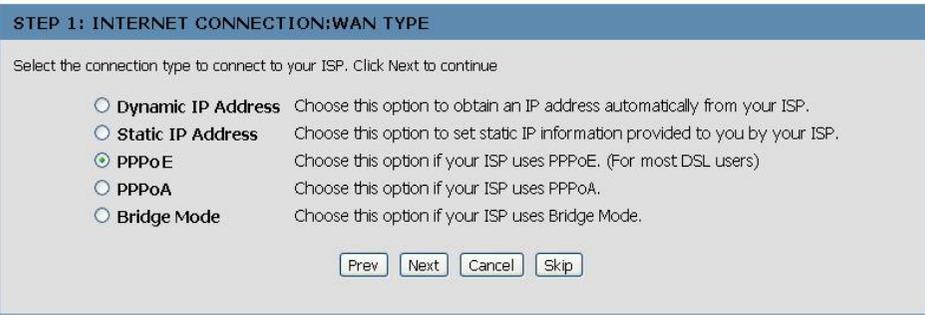
<p>2</p>	<p>Log Info (Información de registro): Información del sistema interno.</p>																																																						
<p>3</p>	<p>USB Info (Información USB): Navegue por el contenido del disco USB adjuntado.</p>																																																						
<p>4</p>	<p>Statistics (Estadísticas): Muestra los paquetes recibidos y transmitidos que atraviesan el dispositivo.</p>	 <table border="1" data-bbox="1218 1114 1653 1241"> <thead> <tr> <th rowspan="2">Interface</th> <th colspan="4">Transmit</th> <th colspan="4">Receive</th> </tr> <tr> <th>Bytes</th> <th>Pkts</th> <th>Errs</th> <th>Drops</th> <th>Bytes</th> <th>Pkts</th> <th>Errs</th> <th>Drops</th> </tr> </thead> <tbody> <tr> <td>LAN:</td> <td>5041462</td> <td>36380</td> <td>0</td> <td>0</td> <td>1310386</td> <td>20404</td> <td>0</td> <td>0</td> </tr> <tr> <td>WAN:</td> <td>946531</td> <td>17630</td> <td>0</td> <td>0</td> <td>46446137</td> <td>32171</td> <td>0</td> <td>0</td> </tr> <tr> <td>Wireless:</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>WLAN_5900</td> <td>0</td> <td>17365</td> <td>0</td> <td>0</td> <td>12503849</td> <td>97733</td> <td>0</td> <td>0</td> </tr> </tbody> </table>	Interface	Transmit				Receive				Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops	LAN:	5041462	36380	0	0	1310386	20404	0	0	WAN:	946531	17630	0	0	46446137	32171	0	0	Wireless:									WLAN_5900	0	17365	0	0	12503849	97733	0	0
Interface	Transmit				Receive																																																		
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops																																															
LAN:	5041462	36380	0	0	1310386	20404	0	0																																															
WAN:	946531	17630	0	0	46446137	32171	0	0																																															
Wireless:																																																							
WLAN_5900	0	17365	0	0	12503849	97733	0	0																																															

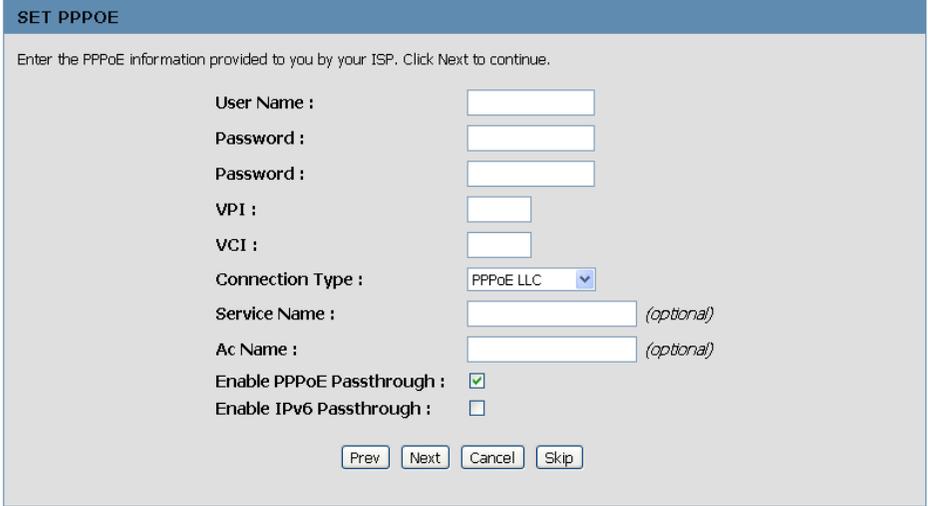
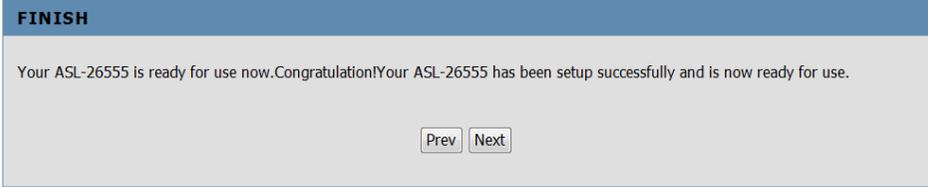
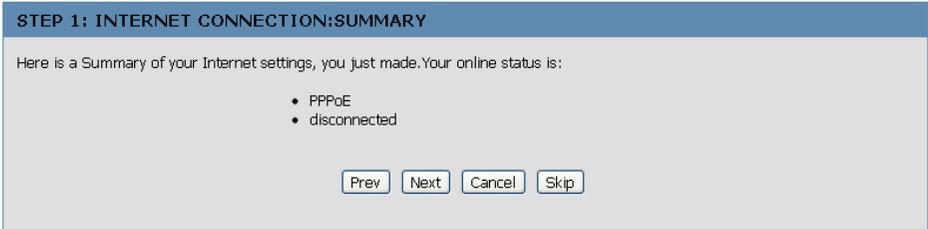
Capítulo 7: Configuración del ASL-26555 para Internet

Descripción general

El ASL-26555 cuenta con un completo Asistente de configuración. El manual contiene una explicación pormenorizada en cada ventana sobre cómo configurar el hardware y el software. Lea todas las instrucciones que siguen con atención y sígalas.

<p>Paso 1:</p>	<p>Haga clic en el Setup Wizard (Asistente de configuración).</p>	
<p>Paso 2:</p>	<p>El asistente ofrece información muy valiosa para empezar.</p>	
<p>Paso 3:</p>	<p>Siga las instrucciones que le guiarán a través del Asistente y haga clic en Next (Siguiete).</p>	

<p>Paso 4:</p>	<p>Siga las instrucciones que se describen en el Asistente y haga clic en Next.</p>	
<p>Paso 5:</p>	<p>Siga las instrucciones del Asistente o la descripción del Capítulo 4 y haga clic en Next.</p>	
<p>Paso 6:</p>	<p>Seleccione el tipo de conexión a su ISP.</p> <p> En la mayoría de los casos, seleccione PPPoE pero si le indica otra cosa, seleccione su preferencia y haga clic en Next.</p>	

<p>Paso 7:</p>	 <p>Puede obtener esta información de su ISP.</p> <ul style="list-style-type: none"> ● Introduzca su User Name ● Introduzca la Password ● Verifique o repita la Password ● VPI & VCI (suministrado por su ISP) ● Connection Type (Tipo de conexión) (suministrado por su ISP) ● Service Name (Nombre de servicio) (suministrado por su ISP) ● AC Name (Nombre de cuenta) (suministrado por su ISP) ● Haga clic en Enable PPPoE Passthrough (Permitir paso PPPoE) <p>Haga clic en Next.</p>	
<p>Paso 8:</p>	<p>Aparecerá la ventana FINISH (Terminar) notificando al usuario que la operación se ha completado con éxito. Haga clic en Next para continuar.</p>	
<p>Paso 9:</p>	<p>Aparecerá un SUMMARY (Resumen) de la configuración. Haga clic en Next para ir a la Wireless Setup (Configuración inalámbrica).</p>	



IMPORTANTE: Si el ASL-26555 no está conectado a un proveedor de servicios de Internet (ISP) válido, el **Resumen de la conexión a Internet** ofrecerá un resumen desconectado tal y como se ve a continuación:

Capítulo 8: Configuración del ASL-26555 para la conectividad inalámbrica

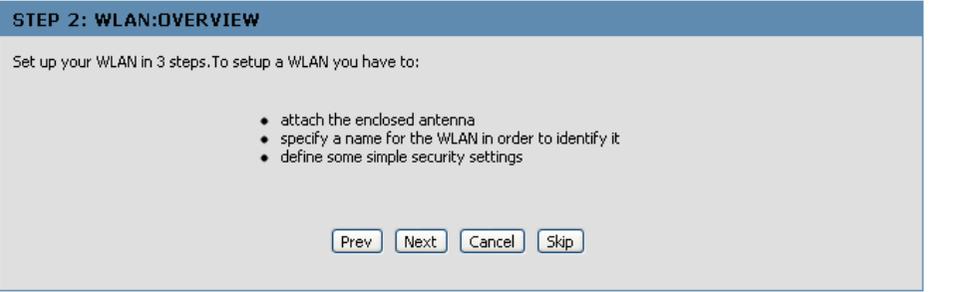
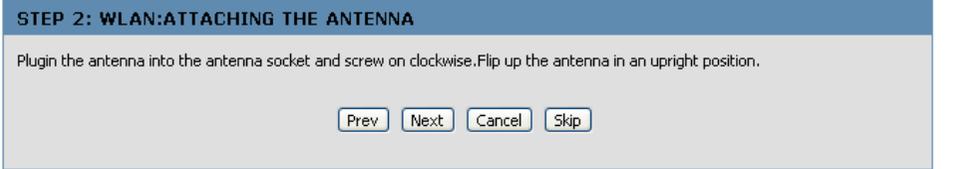
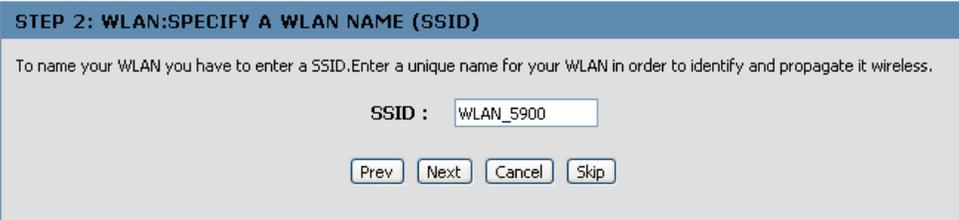
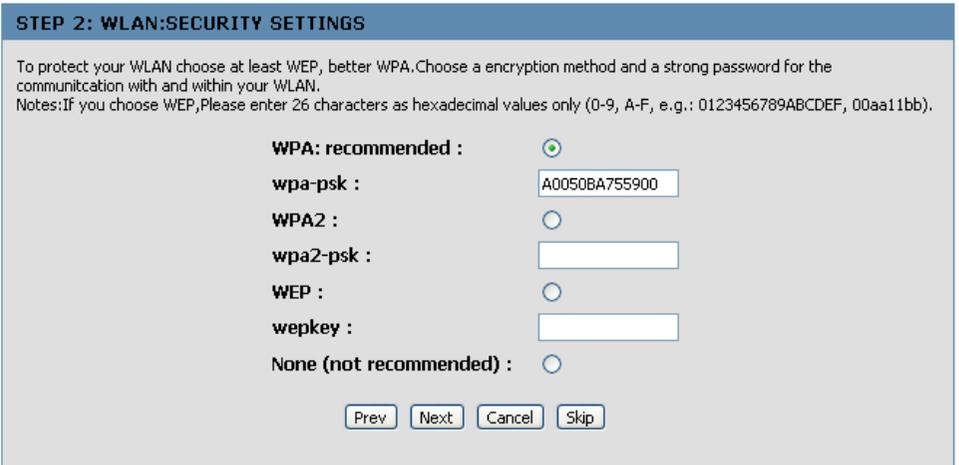
Descripción general

El ASL-26555 cuenta con un completo Asistente de configuración. El manual ofrece una explicación detallada en cada ventana sobre cómo configurar el hardware y el software. Lea atentamente todas las instrucciones y sígalas. El ASL-26555 puede configurarse para funcionar como un punto de acceso inalámbrico. Ofrece una conectividad de hasta 30 metros.



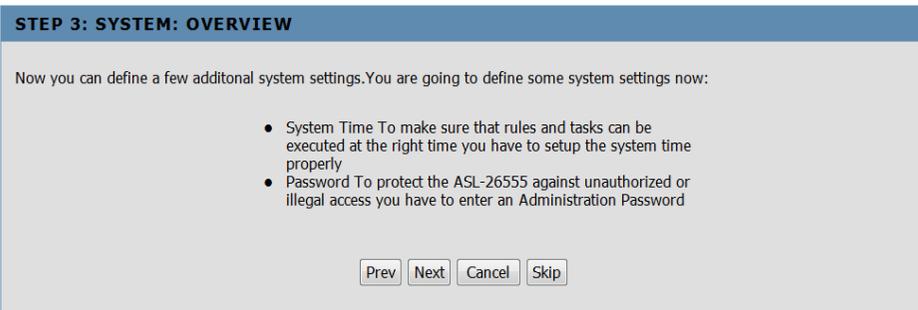
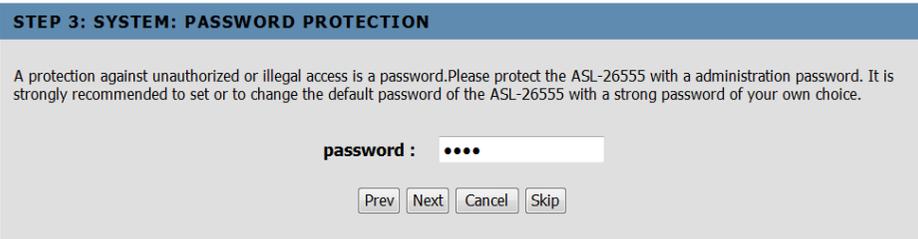
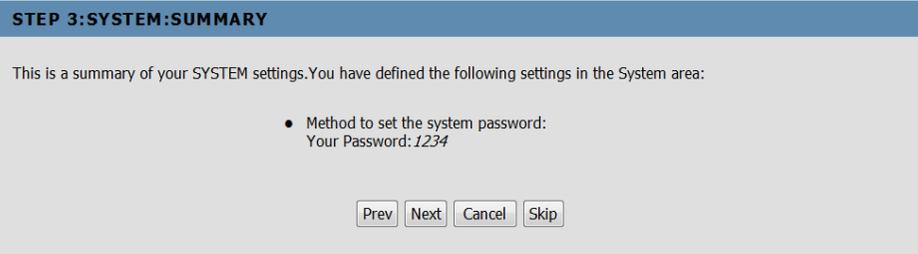
IMPORTANTE: Si no ha llegado a esta fase del Asistente de configuración, consulte el Capítulo 13 para obtener ayuda.

<p>Paso 1:</p>	<p>Haga clic en Next cuando haya completado la configuración ADSL.</p>	
-----------------------	---	--

<p>Paso 2:</p>	<p>El Asistente le ofrecerá una visión general de la conexión de las antenas. Siga las instrucciones de hardware y haga clic en Next.</p>	
<p>Paso 3:</p>	<p>El Asistente le dará instrucciones sobre cómo conectar las antenas para permitir la funcionalidad inalámbrica. Haga clic en Next.</p>	
<p>Paso 4:</p>	<p>Introduzca una ID inalámbrica. Esa SSID es el nombre que utilizará para conectar otros PC al ASL-26555. Haga clic en Next.</p>	
<p>Paso 5:</p>	<p>Seleccione el tipo de configuración de seguridad que desea. Haga clic en Next.</p> <p> Carecer de una configuración de seguridad hace al ASL-26555 vulnerable a los ataques desde el exterior y permite que cualquier usuario pueda acceder al dispositivo de forma inalámbrica.</p> <p> En el Capítulo 2 de este Manual encontrará una lista de las definiciones de seguridad y sus explicaciones.</p>	

<p>Paso 6:</p>	<p>La LAN inalámbrica (WLAN) ya se ha completado. La ventana de resumen le ofrece información sobre los datos introducidos durante la configuración. Haga clic en Next para pasar a la Descripción general (Overview).</p>	
-----------------------	--	---

La parte final del Asistente de configuración ofrece información básica sobre el propio dispositivo.

<p>Paso 7:</p>	<p>Esta pantalla ofrece una descripción general del sistema y le pide que cree una contraseña para todo el sistema. Haga clic en Next para avanzar.</p>	
<p>Paso 8:</p>	<p>El ASL-26555 pide al usuario que introduzca una contraseña para el dispositivo.</p>	
<p>Paso 9:</p>	<p>La pantalla final ofrece un resumen del sistema y muestra la contraseña.</p>	



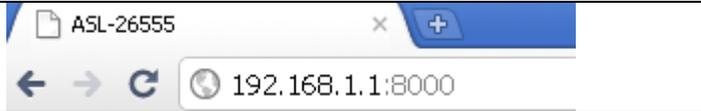
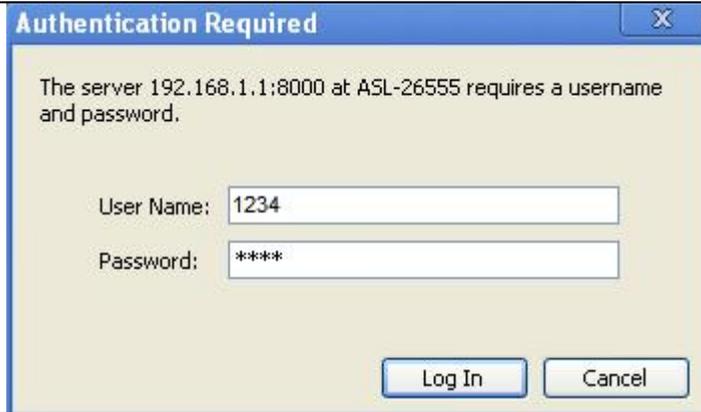
IMPORTANTE: Comprobar el estado del sistema es sencillo. Haga clic en Estado (nº 4 en **Navegar por la pantalla principal**). Esta pantalla ofrece una visión completa del ASL-26555. Sigue un ejemplo.

ASL-26555 //	SETUP	ADVANCED	MAINTENANCE	STATUS	HELP
Device Info LOG Info USB Info Statistics Logout Zoom Level: Middle ▾ Reboot	DEVICE The Device Status page allows you to check the status of your Internet connection, Wireless LAN and LAN.				Helpful Hints.. All of your WAN and LAN connection details are displayed here. More...
GENERAL Current Time : 12/31/1999 19:00:50 Uptime : 0 Day 0 Hour 0 Min 51 Seconds ADSL Firmware Version : v1.0 Firmware Version : v1.1.0.10_PE					
INTERNET STATUS Virtual Circuit : PVC1 ▾ <input type="button" value="Connect"/> <input type="button" value="Disconnect"/> Status : connected Connection Type : PPPoE Uptime : 0 Day 0 Hour 0 Min 7 Seconds IP Address : 59.104.116.139 Subnet Mask : 255.255.255.255 Default Gateway : 59.104.116.1 DNS Server : 200.48.225.130 200.48.225.146					

Capítulo 9: Configuración del ASL-26555 para la conectividad 3G

Overview (Descripción general)

El ASL-26555 cuenta con un completo Asistente de configuración. El manual ofrece una explicación detallada en cada ventana sobre cómo configurar el hardware y el software. Lea atentamente todas las instrucciones y síguelas. El ASL-26555 puede configurarse para funcionar como un punto de acceso 3G. El punto de acceso 3G sustituye a la conexión ADSL normal y ofrece una conexión a Internet móvil y rápida. El dispositivo USB que se incluye en este paquete debe contener también la tarjeta SIM para activar el adaptador USB 3G. Si no es así, póngase en contacto con el vendedor o devuelva el producto.

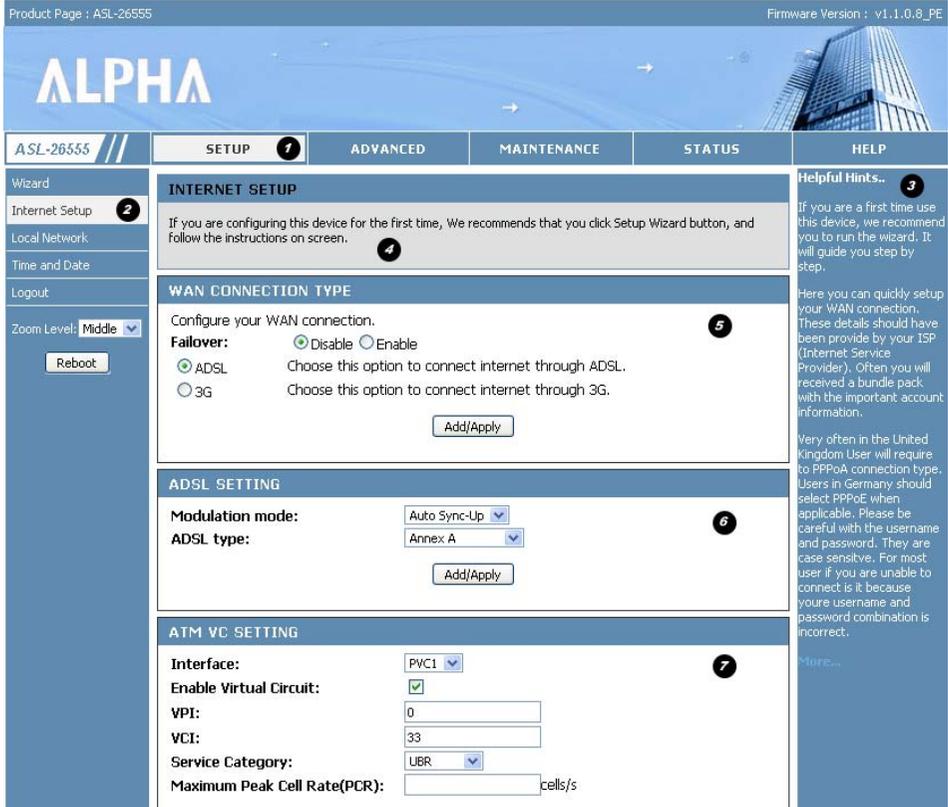
Paso 1:	Escriba la dirección IP por defecto en la barra de herramientas de navegación del ASL-26555.	
Paso 2:	Escriba su Nombre de usuario y su Contraseña y haga clic en Log In .	
Paso 3:	En Configuración, haga clic en Internet Setup (Configuración de Internet)	
Paso 4:	En WAN Connection Type (Tipo de conexión WAN) , haga clic en el botón circular 3G y haga clic en Add/Apply (Añadir/Aplicar) para realizar los cambios.	

Paso 5:	En 3G INTERNET CONNECTION (Conexión a Internet 3G) , introduzca la información necesaria suministrada por su proveedor de servicios.	<div style="border: 1px solid black; padding: 5px;"> <div style="background-color: #4f81bd; color: white; padding: 2px;">3G INTERNET CONNECTION</div> <p>User Name: <input type="text"/></p> <p>Password: <input type="password"/></p> <p>Dial Number: <input type="text" value="*99#"/></p> <p>APN: <input type="text" value="internet"/></p> <p>PIN Code: <input type="text"/> (optional)</p> <p>Reconnect Mode: <input checked="" type="radio"/> Always-on <input type="radio"/> Connect-on demand</p> <p>Maximum Idle Time: <input type="text" value="2"/> (minutes, 0-infinite)</p> <p>MTU: <input type="text" value="1492"/></p> </div>
Paso 6:	Haga clic en Add/Apply	<div style="border: 1px solid black; padding: 5px; text-align: center;"> <input type="button" value="Add/Apply"/> </div>
Paso 7:	 <p>IMPORTANTE: Lea el aviso del botón Add/Apply. Dice: “Vaya a MAINTENANCE->System Settings (MANTENIMIENTO->Configuración del sistema) y haga clic en el botón Reboot (Reiniciar) para reiniciar el dispositivo y hacer que sean efectivos los nuevos ajustes”.</p>	<p>Note:Go to MAINTENANCE -> System Settings and click the Reboot button to restart the device and let your new settings take effect!</p>

Capítulo 10: Configuración de Internet

Descripción general

El ASL-26555 cuenta con un Asistente de configuración que permite configurar la conexión a Internet sin ningún otro tipo de instalación adicional. Esta configuración puede ser utilizada tanto por legos como por profesionales. Los usuarios también pueden manipular determinados ajustes al configurar o diagnosticar problemas en la sección Configuración de Internet. En este breve capítulo, vamos a repasar lo que ha creado el Asistente y lo que puede configurarse por separado. En la pestaña **Configuración** (1), haga clic en **Configuración de Internet** (2). El archivo de ayuda de la ventana derecha es muy útil. Utilícelo como acompañamiento a este manual o como una lista de definiciones.

<p>El WAN CONNECTION TYPE (TIPO DE CONEXIÓN WAN), (5), permite al usuario configurar los ajustes de la WAN.</p>	<p>Seleccione ADSL para las conexiones de cable o 3G para la conectividad móvil. Seleccione Enable (Habilitar) recuperación de fallos para que el dispositivo 3G actúe como respaldo del dispositivo ADSL en caso de producirse un fallo del primero y viceversa. Haga clic en Add/Apply cuando haya terminado.</p>	
<p>En ADSL SETTINGS (AJUSTES ADSL) (6)</p>	<p>Seleccione el Modulation mode (Modo de modulación) y el ADSL Type (Tipo de ADSL). Esta información se la suministrará su ISP</p>	
<p>En ATM VC SETTINGS (AJUSTES ATM VC)</p>	<p>Seleccione los ajustes apropiados. Contacte con su ISP para obtener los detalles. Cada país y cada región varía. Busque las definiciones en la sección Ayuda.</p>	

<p>Toda o la mayoría de la información necesaria para los WAN SETTINGS (8) y WAN (9) se la suministrará su proveedor de servicios de Internet (ISP). Consulte sus instrucciones.</p>	<p>En WAN SETTINGS (AJUSTES WAN) (8), seleccione uno de los protocolos suministrados por su ISP (habitualmente es PPPoE).</p>
<p>En WAN (9),</p>	<p>Escriba el Nombre de usuario y la Contraseña que le haya dado su ISP. EL tipo de conexión suele ser PPPoE pero puede variar en función del ISP.</p> <p>El Service Name (Nombre de servicio) y el Nombre de cuenta son opcionales.</p> <p>El IP Control (Control IP) depende de las instrucciones del ISP.</p> <p>Escriba una Static IP Address (Dirección IP estática) si es preciso.</p> <p>Seleccione un PPPoE Type (Tipo de PPPoE) en el menú desplegable.</p> <p>La información de la interfaz unnumbered LAN/IP/Netmask (LAN/IP/máscara de red no numerada) depende de las especificaciones de su ISPc.</p> <p>MTU está configurado por defecto.</p> <p>Haga clic en AutoDNS si desea habilitarlo.</p> <p>Seleccione Default Route (Ruta por defecto) en Usage (Uso) dentro de la lista desplegable.</p> <p>Habilita Network Address Translation (Traducción de direcciones de red) (NAT) para que pueda utilizar dispositivos internos para acceder a</p>

WAN SETTINGS

Configure your DSL connection here. Please consider the information of your provider on the settings otherwise it may not be possible to establish a connection. 8

Dynamic IP Address Choose this option to obtain an IP address automatically from your ISP. (For most Cable modem users)

Static IP Address Choose this option to set static IP information provided to you by your ISP.

PPPoE Choose this option if your ISP uses PPPoE. (For most DSL users)

PPPoA Choose this option if your ISP uses PPPoA. (For most DSL users)

Bridge Mode Choose this option if your ISP uses Bridge.

WAN

9

Username:

Password:

Confirm Password:

Connection Type:

Service Name: (optional)

AC name: (optional)

IP Control:

Static IP Address:

PPPoE Type :

Unnumbered LAN Interface :

Unnumbered IP:

Unnumbered Netmask:

MTU:

AutoDns:

Usage:

NAT Enable:

IGMP Enable:

Enable PPPoE Passthrough:

Enable IPv6 Passthrough:

Authentication Protocol:

Connect mode select:
 Always-on
 Connect-on demand

Maximum Idle Time: Minutes

	Internet.	
	Deje IGMP en blanco.	
	Marque Enable PPPoE Passthrough (Habilitar paso PPPoE) pero deje Habilitar paso IPv6 (Enable IPv6 Passthrough) en blanco.	
	Si su proveedor de servicios utiliza protocolos de autenticación, habilite PAP y CHAP en el dispositivo.	
	Haga clic en el botón circular Always-on (Siempre activado) en Connect mode select (Selección de modo de conexión) para mantener el dispositivo activo.	
	Escriba una hora en minutos para determinar si quiere que el dispositivo se desconecte cuando haya estado un tiempo inactivo.	
	Haga clic en Add/Apply cuando haya terminado.	

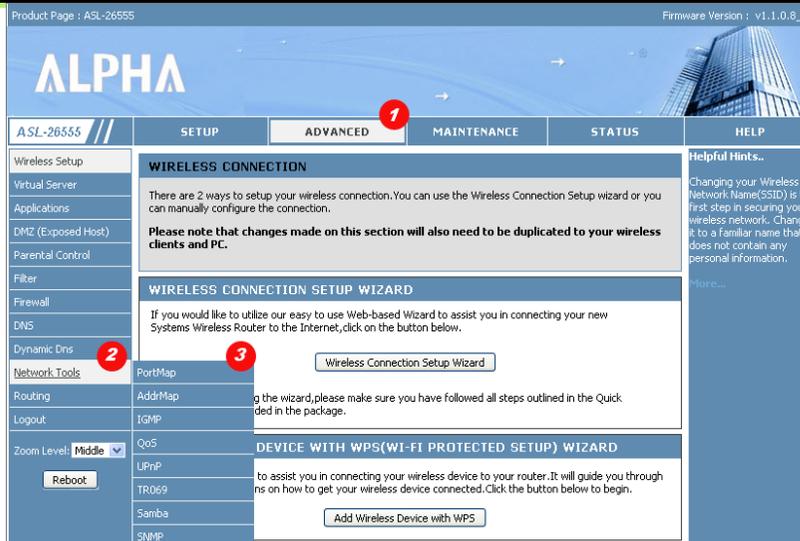
Capítulo 11: Configuración de la red local

Descripción general

El ASL-26555 puede actuar como router para dispositivos conectados a sus puertos Ethernet. Cuenta con su propia tabla de direcciones IP. También actúa como servidor DHCP por lo que puede actuar como repartidor o servidor de direcciones IP con los dispositivos conectados. En este capítulo veremos cómo habilitar la configuración DHCP y determinar los ajustes de conexión.

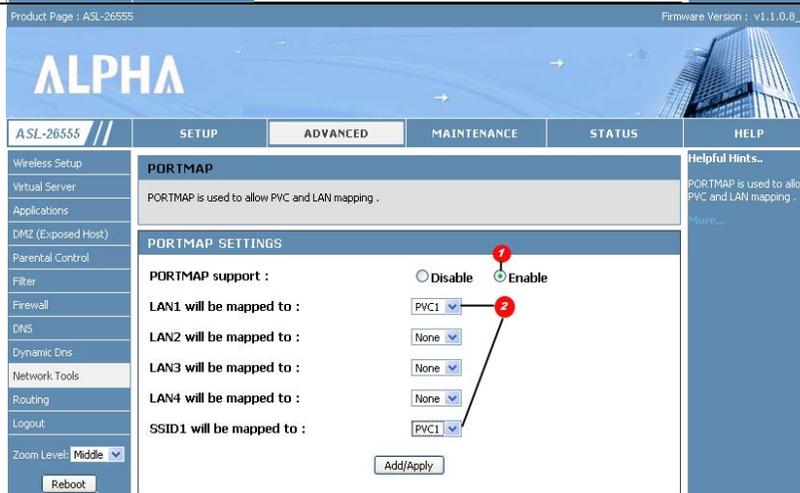
Router Settings (Configuración del router):	<p>De acuerdo con las instrucciones de la ventana de Configuración del router, es recomendable no modificar la Dirección IP del router. Si se cambia esta IP puede provocarse un defecto en la máquina o resetearse el dispositivo a los valores de fábrica. Las máscaras de subred no pueden ser iguales. Cuando haya terminado, haga clic en el botón Add/Apply que se encuentra justo debajo del campo Habilitar servidor DHCP.</p>	<div data-bbox="831 491 1944 959"> <p>ROUTER SETTINGS</p> <p>Use this section to configure the local network settings of your router. The IP Address that is configured here is the IP Address that you use to access the Web-based management interface. If you change the IP Address here, you may need to adjust your PC's network settings to access the network again.</p> <p>Router IP Address : <input type="text" value="192.168.1.1"/></p> <p>Subnet Mask : <input type="text" value="255.255.255.0"/></p> <p><input type="checkbox"/> Configure the second IP Address and Subnet Mask for LAN interface</p> <p>IP Address : <input type="text" value="10.167.64.81"/></p> <p>Subnet Mask : <input type="text" value="255.255.255.248"/></p> </div>
DHCP ENABLE / DISABLE LAN PORT (HABILITAR / DESHABILITAR PUERTO LAN DHCP):	<p>De acuerdo con la notificación, este campo sólo trabajará si el mapeo de puertos está habilitado.</p>	<div data-bbox="831 1067 1944 1281"> <p>DHCP ENABLE / DISABLE LAN PORT</p> <p><i>Notice: This function is effective when portmap is enabled. And port# must be mapped to PVC which is not in bridge mode.</i></p> <p>LAN port : port1 <input checked="" type="checkbox"/> port2 <input checked="" type="checkbox"/> port3 <input checked="" type="checkbox"/> port4 <input checked="" type="checkbox"/></p> </div>

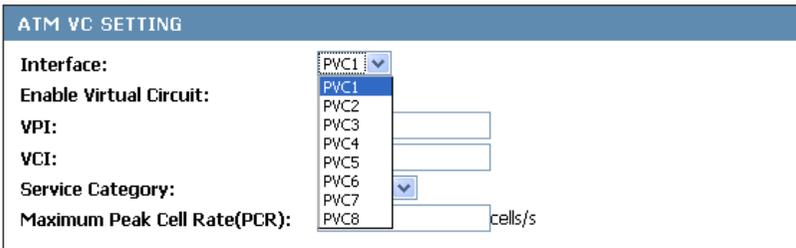
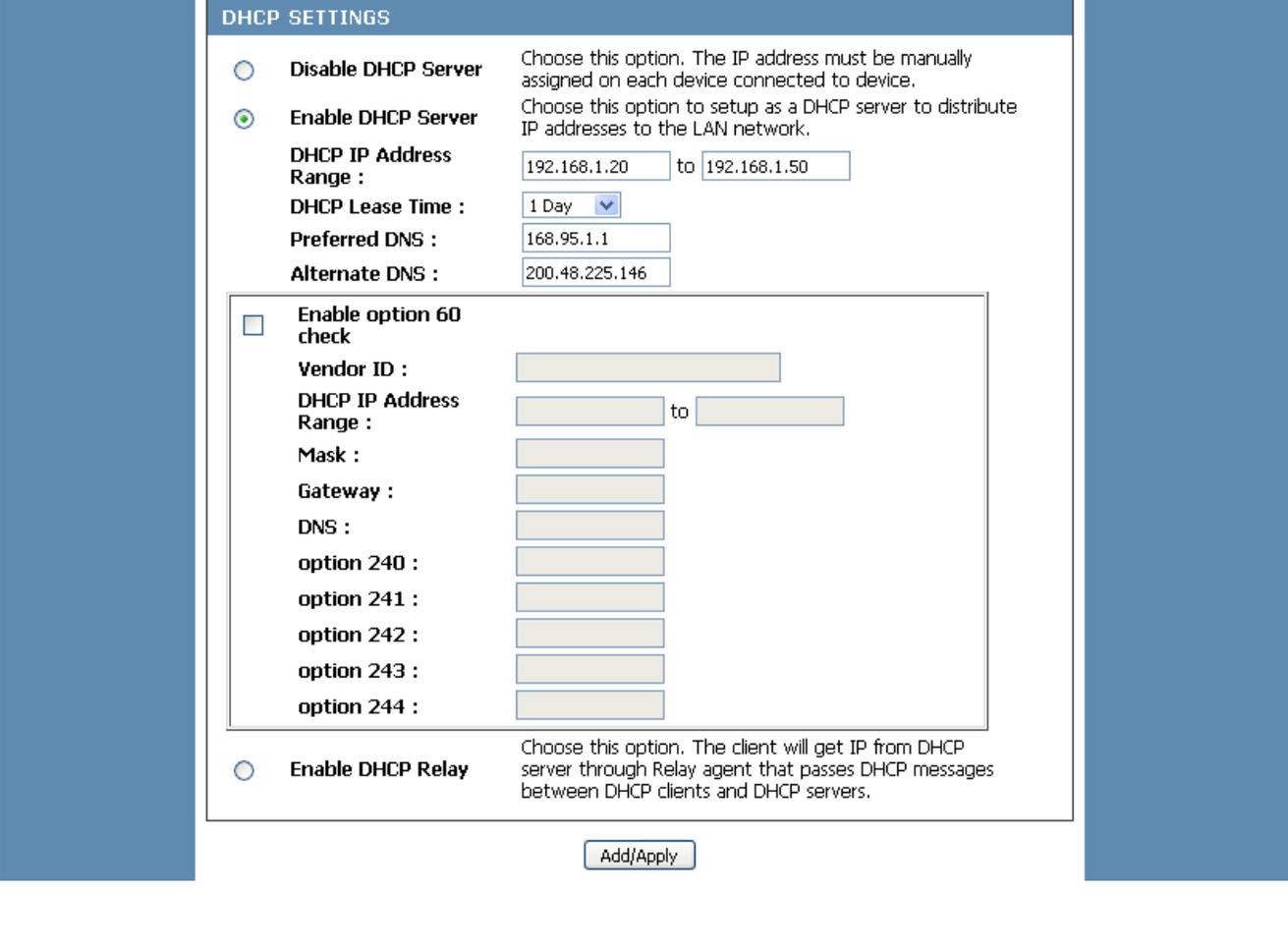
Para habilitar el mapeo de puertos, vaya a la pestaña **Advanced** tab, **Network Tools**, **PortMap** (**Avanzado, Herramientas de red, PortMap**).



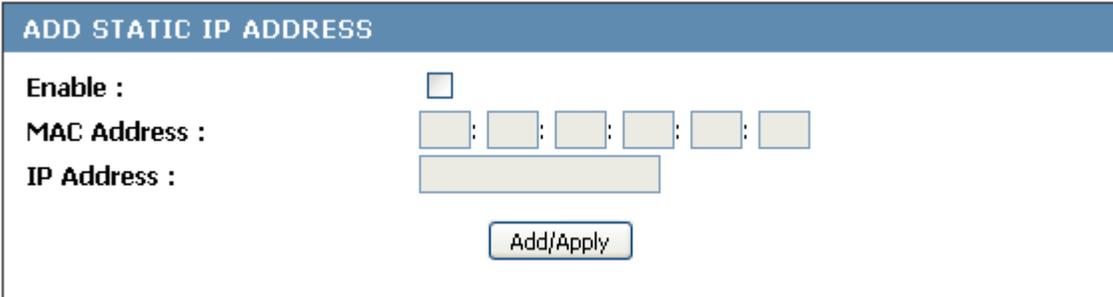
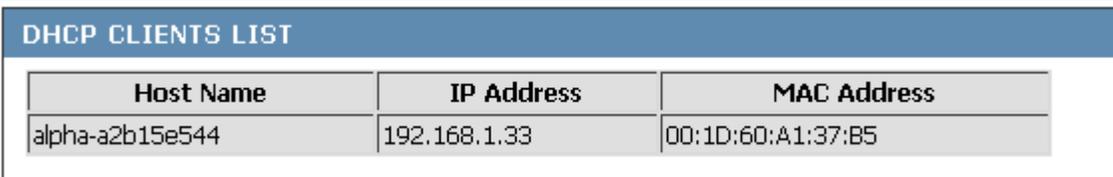
En **PORTMAP SETTINGS** (**CONFIGURACIÓN PORTMAP**)

Haga clic en el botón circular **Enable**. Seleccione el puerto Ethernet que desea mapear y en la lista desplegable seleccione PVC1, luego haga clic en **Add/Apply**.



	<p> IMPORTANTE: Los ajustes de PVC1 se configuran en Setup, Internet Setup, ATM VC Setting .</p>	
<p>DHCP SETTINGS (CONFIGURACIÓN DHCP):</p>	<p>El ASL-26555 también puede actuar como servidor DHCP. En otras palabras, puede asignar a los dispositivos conectados direcciones IP a partir de su propia tabla de enrutamiento IP.</p> <p>Haga clic en Disable DHCP server si no quiere que el ASL-26555 emita direcciones IP internas.</p> <p>Haga clic en Enable DHCP server si desea que el ASL-26555 emita direcciones IP.</p> <p>El DHCP IP Address Range (Rango de direcciones IP DHCP) es un conjunto de números dentro de la misma pila. El rango final puede estar entre 1 y 99.</p> <p>Seleccione un tiempo de conexión en la lista desplegable DHCP Lease</p>	

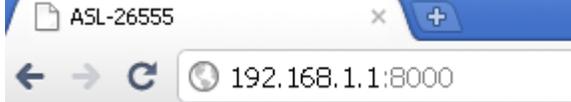
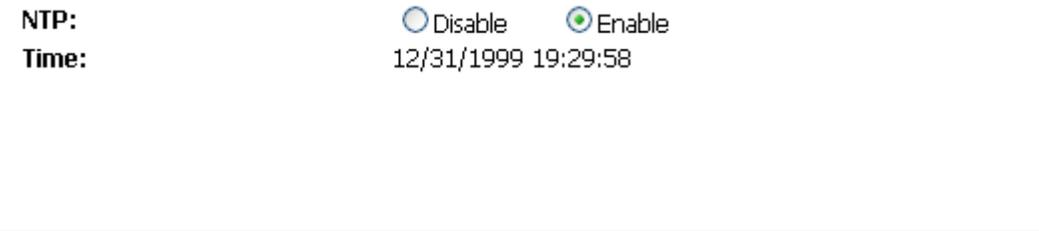
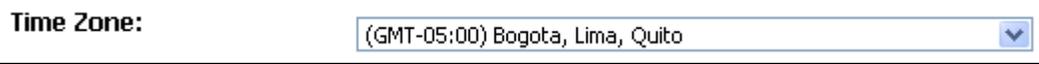
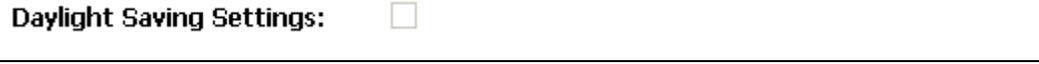
	<p>Time (Tiempo de conexión DHCP). Indica durante cuánto tiempo permanecerá activa la dirección IP.</p> <p>Escriba el DNS preferido asignado y la DNS alternativo.</p> <p>Marque Enable option 60 (Habilitar opción 60). Este método permite a un servidor DHCP diferenciar entre los dos tipos de máquinas cliente y procesar las solicitudes de los dos tipos de módems correctamente.</p> <p>El resto de la información lo suministrará su ISP o distribuidores terceros.</p> <p>Proceda igual para el resto de las opciones si fuera preciso.</p>	<div style="border: 1px solid black; padding: 10px;"> <input type="checkbox"/> Enable option 60 check Vendor ID : <input type="text"/> DHCP IP Address Range : <input type="text"/> to <input type="text"/> Mask : <input type="text"/> Gateway : <input type="text"/> DNS : <input type="text"/> option 240 : <input type="text"/> option 241 : <input type="text"/> option 242 : <input type="text"/> option 243 : <input type="text"/> option 244 : <input type="text"/> </div>
	<p>Haga clic en Enable DHCP Relay (Habilitar DHCP Relay). Marque esta opción si está trabajando a través de un agente DHCP relay. Haga clic en Add/Apply cuando haya terminado.</p>	<p><input type="radio"/> Enable DHCP Relay Choose this option. The client will get IP from DHCP server through Relay agent that passes DHCP messages between DHCP clients and DHCP servers.</p>

<p>Add Static IP Address (Añadir dirección IP estática)</p>	<p>Marque la casilla de verificación para habilitar esta opción. Escriba la dirección MAC y la dirección IP del dispositivo que desea activar. Haga clic en Add/Apply.</p>	
<p>DHCP RESERVATIONS LIST (LISTA DE RESERVAS DHCP)</p>	<p>En esta área aparecerán la lista de dispositivos reservados (su dirección IP no podrá ser asignada a otros). Puede eliminar cualquier dispositivo seleccionándolo y haciendo clic en Remove selected (Eliminar selección).</p>	
<p>DHCP CLIENTS LIST (LISTA DE CLIENTES DHCP)</p>	<p>El ASL-26555 aparece en la lista y pueden eliminarse otros dispositivos si éste se conecta o añade.</p>	

Capítulo 12: Configuración de la hora y la fecha

Descripción general

El ASL-26555 mantiene su propio registro temporal. Esto quiere decir que es capaz de sincronizarse con todos los dispositivos conectados. Siga esta sencilla guía para configurar la hora y al fecha.

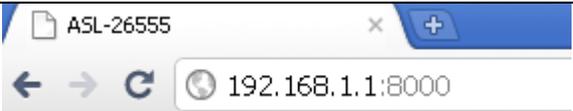
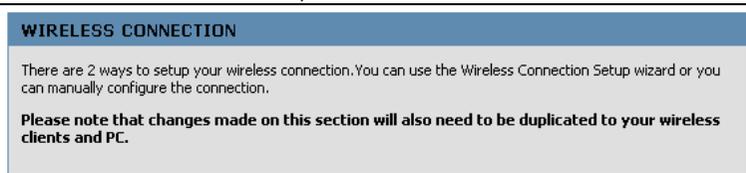
TIME SETTINGS:	Escriba la dirección IP y el puerto por defecto en la barra de herramientas de navegación del ASL-26555.	
Paso 1:	Introduzca su Nombre de usuario y su Contraseña y haga clic en Log In .	
Paso 2:	En SETUP , haga clic la pestaña Time and date (Hora y fecha) en la barra de la izquierda.	
Paso 3:	En primer lugar vamos a describir la configuración de la hora. Haga clic en Enable para iniciar el Network Time Protocol (Protocolo de tiempo de red NTP) . El dispositivo dará automáticamente la hora y la fecha.	
Paso 4:	Seleccione Time zone (Zona horaria) .	
Paso 5:	Seleccione Daylight Savings (Ahorro de luz diurna) si fuera preciso.	

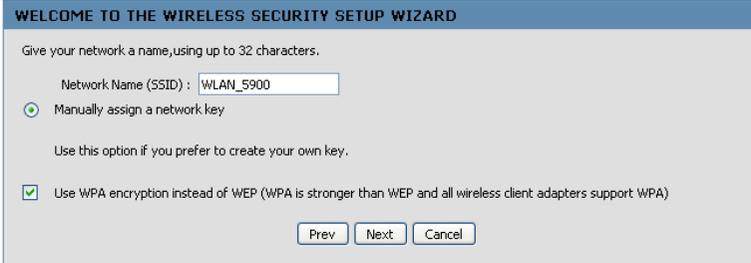
Paso 6:	Introduzca sus Network Time Protocol Servers (Servidores de protocolo de tiempo de red) y haga clic en Add/Apply .	Primary NTP server : <input data-bbox="1491 161 1729 197" type="text" value="time.windows.com"/> Secondary NTP server : <input data-bbox="1491 204 1729 240" type="text" value="time.nist.gov"/> <input data-bbox="1583 272 1729 309" type="button" value="Add/Apply"/>
----------------	--	---

Capítulo 13: Configuración de la conexión inalámbrica

Descripción general

Si no ha seguido el Asistente de configuración inalámbrica en el Capítulo 8, este capítulo le resultará útil para configurar todas las conexiones inalámbricas. El ASL-26555 puede conectar muchos PC y dispositivos. El Asistente de configuración inalámbrica es la forma más sencilla de conectar sin cables el router y puede encontrarse también en la ventana Avanzado => Configuración inalámbrica. Sin embargo, si tiene que añadir o eliminar dispositivos, este procedimiento le resultará familiar cuando haya leído este capítulo.

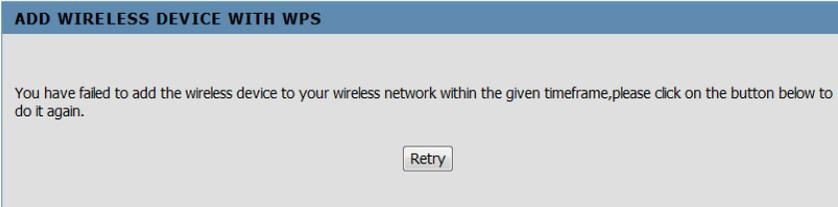
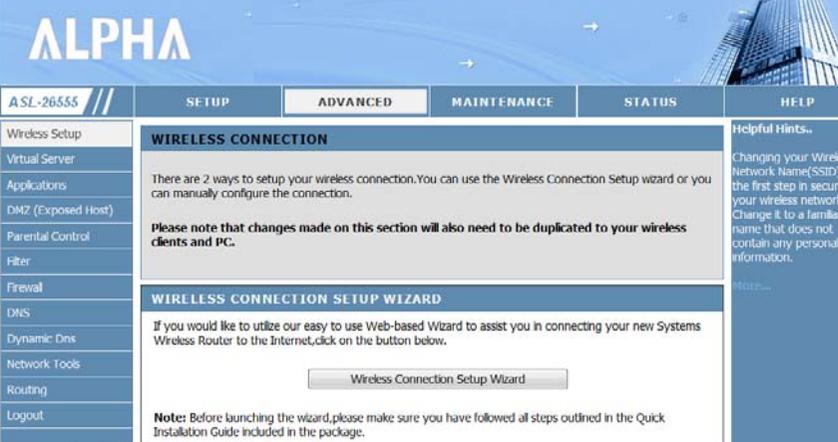
Paso 1:	Abra el navegador y escriba la dirección IP por defecto del ASL-26555.	
Paso 2:	Escriba su Nombre de usuario y su Contraseña y haga clic en Log In .	
Paso 3:	Haga clic en Avanzado, Configuración inalámbrica.	
Paso 4:	Sigue una descripción de la configuración inalámbrica:	

<p>Paso 5:</p>	<p>⚠ IMPORTANTE: Si ya ha configurado la configuración inalámbrica con el Asistente de configuración inalámbrica, sáltese este paso.</p> <p>Haga clic en el Wireless Connection Setup Wizard (Asistente de configuración inalámbrica)</p>	
<p>Paso 6:</p>	<p>A. Cree un Network Name (Nombre de red) para el dispositivo.</p> <p>B. Haga clic en el botón circular para Manually assign a network key (Asignar manualmente una clave de red).</p> <p>C. Marque Use WPA encryption instead of WEP (Utilizar encriptación WPA en lugar de WEP).</p> <p>D. Haga clic en Next.</p>	
<p>Paso 7:</p>	<p>A. Escriba una Network Key (Clave de red).</p> <p>B. Haga clic en Next.</p>	
<p>Paso 8:</p>	<p>La siguiente ventana muestra un resumen del Nombre de red, Modo de seguridad inalámbrica y la Clave de red. Haga clic en Save (Guardar).</p>	
<p>Paso 9:</p>	<p>La ventana de resumen final confirma los detalles de la configuración.</p>	
<p>Paso 10:</p>	<p>Haga clic en OK para volver a la ventana de configuración inalámbrica principal.</p>	

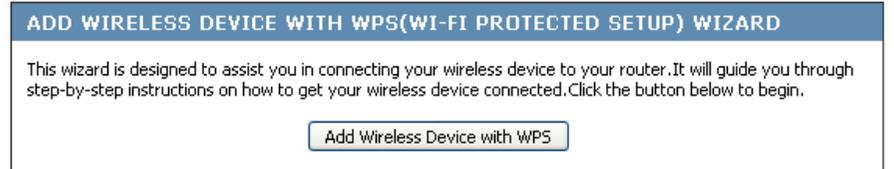
Configuración protegida Wi-Fi

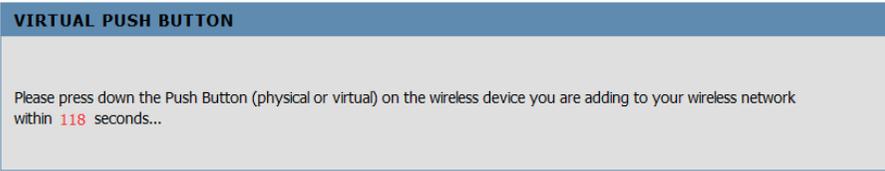
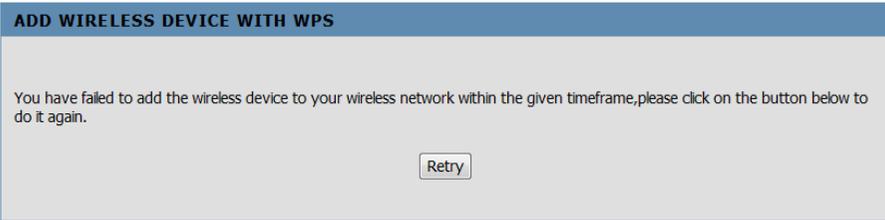
Existen dos formas en las que un usuario puede conectarse usando la Configuración protegida Wi-Fi. Un método es utilizando un PIN y otro es el método PBC. En primer lugar, vamos a revisar la configuración del sistema utilizando un método PIN.

Paso 1:	Haga clic en Advanced => Wireless Setup => Add Wireless Device with WPS (Añadir dispositivo inalámbrico con WPS) .	
Paso 2:	Seleccione Auto y haga clic Next .	
Paso 3:	Ahora introduzca el Número de identificación personal (generado por el cliente inalámbrico) y haga clic en Connect (Conectar) .	
Paso 4:	El dispositivo esperará ahora una respuesta del otro dispositivo.	

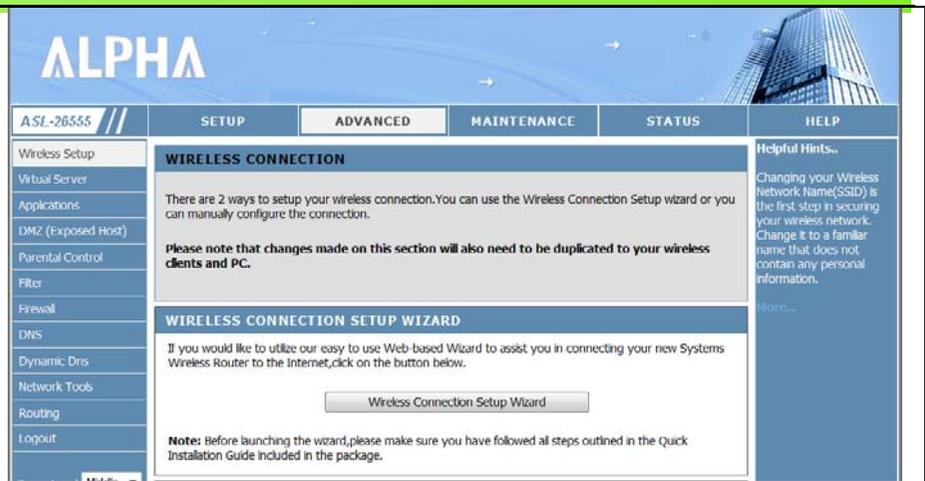
<p>Paso 5:</p>	<p>Si no hay conexión, el dispositivo mostrará esta pantalla.</p>	
<p>Paso 6:</p>	<p>Si se produce una respuesta del dispositivo inalámbrico, el sistema le redirigirá automáticamente a la pantalla principal.</p>	

Ahora vamos a ver cómo configurar el sistema utilizando el método PBC.

<p>Paso 1:</p>	<p>Haga clic en Advanced => Wireless Setup => Add Wireless Device with WPS.</p>	
<p>Paso 2:</p>	<p>Seleccione Auto y haga clic en Next.</p>	

<p>Paso 3:</p>	<p>Haga clic en PBC en el menú y haga clic en Connect (Conectar).</p>	 <p>ADD WIRELESS DEVICE WITH WPS(WI-FI PROTECTED SETUP)</p> <p>There are two ways to add wireless device to your wireless network:</p> <ul style="list-style-type: none"> -PIN(Personal Identification Number) -PBC(Push Button Configuration) <p><input type="radio"/> PIN : <input type="text"/></p> <p>Please enter the PIN from your wireless device and click the below "Connect" button</p> <p><input checked="" type="radio"/> PBC</p> <p>Please press the push button on your wireless device and press the "Connect" button below within 120 seconds</p> <p><input type="button" value="Prev"/> <input type="button" value="Connect"/></p>
<p>Paso 4:</p>	<p>El dispositivo esperará ahora una respuesta del otro dispositivo.</p>	 <p>VIRTUAL PUSH BUTTON</p> <p>Please press down the Push Button (physical or virtual) on the wireless device you are adding to your wireless network within 118 seconds...</p>
<p>Paso 5:</p>	<p>Si no hay conexión, el dispositivo mostrará esta ventana.</p>	 <p>ADD WIRELESS DEVICE WITH WPS</p> <p>You have failed to add the wireless device to your wireless network within the given timeframe,please click on the button below to do it again.</p> <p><input type="button" value="Retry"/></p>

Paso 6: Si se produce una respuesta del dispositivo inalámbrico, el sistema le redirigirá automáticamente a la pantalla principal.



La opción manual para añadir un dispositivo inalámbrico con WPS presenta un enfoque más pormenorizado y también tiene más opciones configurables. Vamos a ver ahora cómo configurarlo manualmente.

Paso 1: Haga clic en **Advanced => Wireless Setup => Add Wireless Device with WPS.**



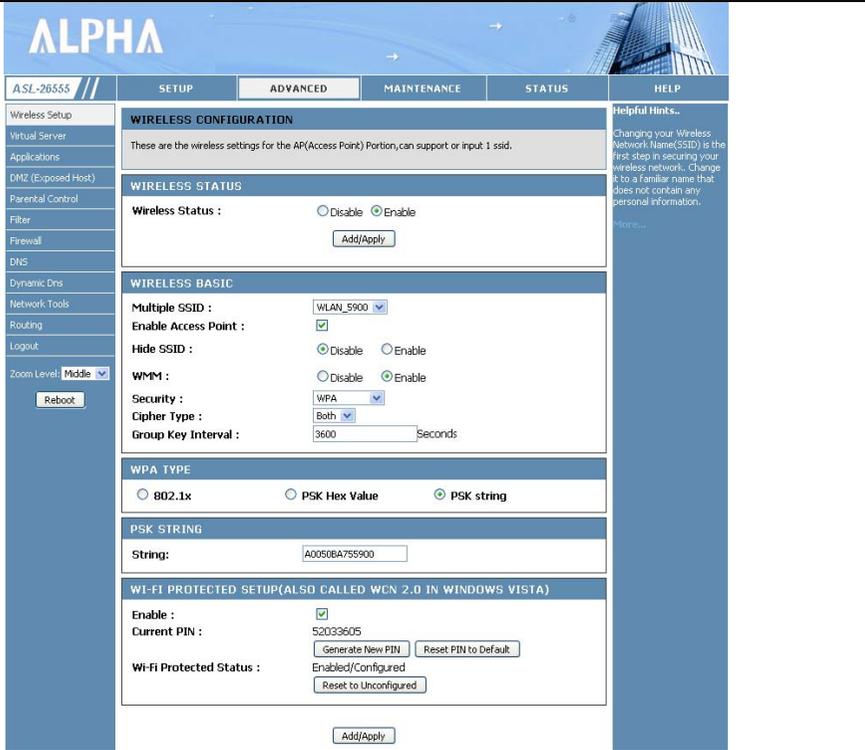
Paso 2: Seleccione **Manual** y haga clic en **Next.**



Paso 3: El dispositivo generará automáticamente información que debe añadirse al dispositivo que se está conectando al ASL-26555. Haga clic en **OK** para continuar.

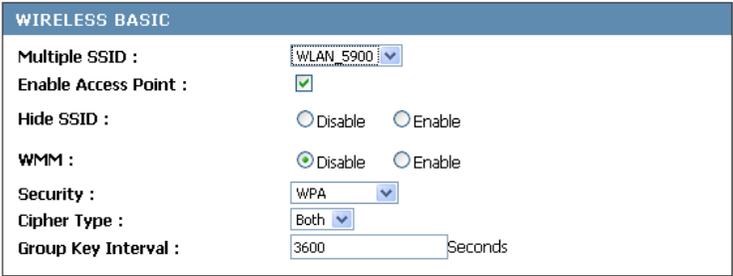
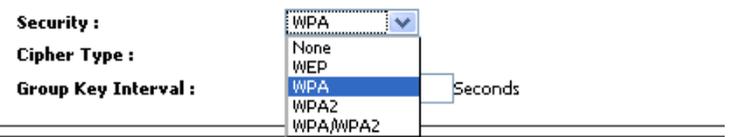
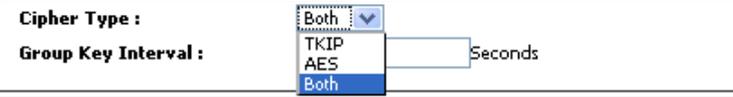
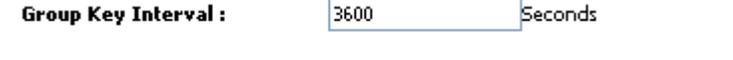
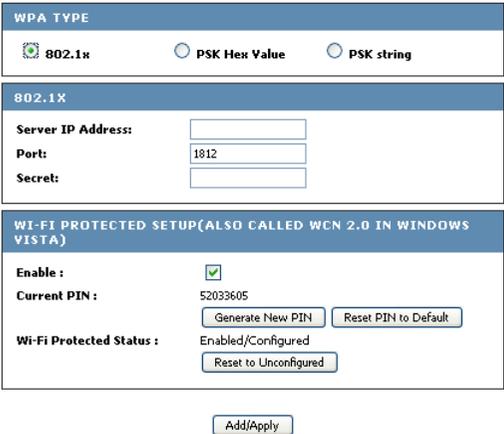


Paso 4: Configure la red inalámbrica en la ventana **Configuración inalámbrica**.



Paso 5: Seleccione **Enable** en la sección **Wireless Status (Estado inalámbrico)** y haga clic en **Add/Apply**.



<p>Paso 6:</p>	<p>En Wireless Basics (Básicos inalámbricos), seleccione el SSID que desea configurar. Marque la casilla Enable Access Point (Habilitar punto de acceso). Haga clic en Disable para ver el SSID en la red. Habilite WMM para reducir el consumo de energía haciendo que los dispositivos móviles accedan al ASL-26555.</p>	
<p>Paso 7:</p>	<p>Seleccione el tipo de Security (Seguridad) en la lista desplegable.</p>	
<p>Paso 8:</p>	<p>Seleccione un Cipher type (Tipo de cifrado). Puede ser TKIP, AES o Both (Ambos).</p>	
<p>Paso 9:</p>	<p>Introduzca una duración del Group Key Interval (Intervalo de claves de grupo). Esto queda a su entera discreción.</p>	
<p>Paso 10:</p>	<p>En WPA Type (Tipo de WPA) seleccione la versión que mejor se ajuste a sus necesidades de seguridad. Las tres posibilidades son 802.1x, Valor hex PSK o Cadena PSK. Si selecciona un tipo de seguridad cambiará el cuadro de abajo dando más opciones al usuario.</p> <p> IMPORTANTE: Las tres opciones se ilustran en las ventanas de la derecha. En función del tipo de WPA que se seleccione, se tendrá un método de configuración diferente. Sigue una breve descripción de los tres tipos de WPA.</p>	

		<div data-bbox="1256 156 1805 236"> <p>WPA TYPE</p> <p><input type="radio"/> 802.1x <input checked="" type="radio"/> PSK Hex Value <input type="radio"/> PSK string</p> </div> <div data-bbox="1256 244 1805 323"> <p>PSK HEX VALUE</p> <p>Hex Value: <input type="text" value="A0050BA755900"/></p> </div> <div data-bbox="1256 331 1805 523"> <p>WI-FI PROTECTED SETUP(ALSO CALLED WCN 2.0 IN WINDOWS VISTA)</p> <p>Enable : <input checked="" type="checkbox"/></p> <p>Current PIN : 52033605 <input type="button" value="Generate New PIN"/> <input type="button" value="Reset PIN to Default"/></p> <p>Wi-Fi Protected Status : Enabled/Configured <input type="button" value="Reset to Unconfigured"/></p> </div> <div data-bbox="1491 547 1574 571"> <p><input type="button" value="Add/Apply"/></p> </div> <div data-bbox="1256 579 1805 659"> <p>WPA TYPE</p> <p><input type="radio"/> 802.1x <input checked="" type="radio"/> PSK Hex Value <input checked="" type="radio"/> PSK string</p> </div> <div data-bbox="1256 667 1805 746"> <p>PSK STRING</p> <p>String: <input type="text" value="A0050BA755900"/></p> </div> <div data-bbox="1256 754 1805 946"> <p>WI-FI PROTECTED SETUP(ALSO CALLED WCN 2.0 IN WINDOWS VISTA)</p> <p>Enable : <input checked="" type="checkbox"/></p> <p>Current PIN : 52033605 <input type="button" value="Generate New PIN"/> <input type="button" value="Reset PIN to Default"/></p> <p>Wi-Fi Protected Status : Enabled/Configured <input type="button" value="Reset to Unconfigured"/></p> </div> <div data-bbox="1491 970 1574 994"> <p><input type="button" value="Add/Apply"/></p> </div>
--	--	--

Comprender los tipos de WPA

802.1x es sencillamente un estándar para transmitir EAP en una LAN tanto con cables como inalámbrica. Se trata básicamente de autenticación y nada más.

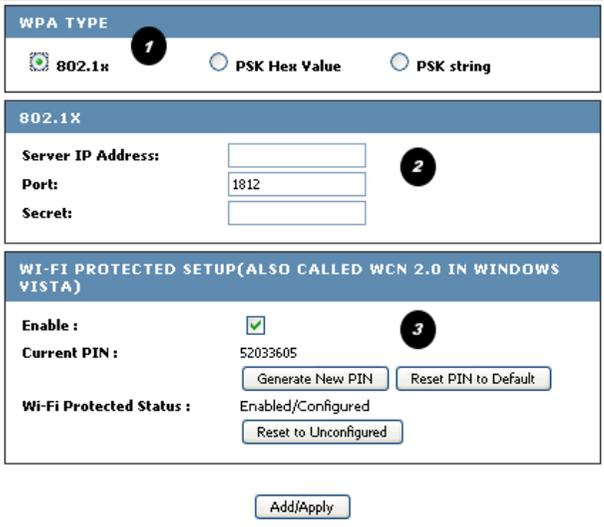
802.1x emplea tres términos que son importantes:

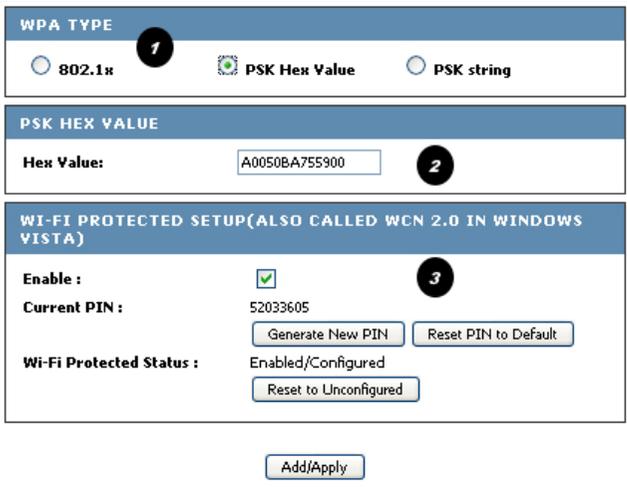
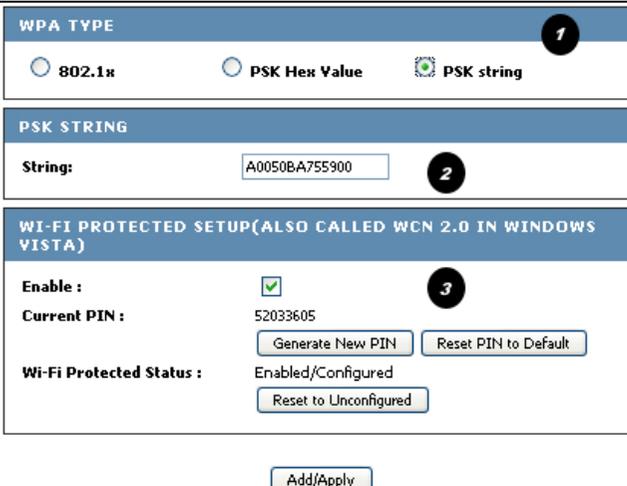
1. El usuario o cliente que desea autenticarse.
2. El servidor que realiza la autenticación.
3. El dispositivo entre ellos, como el ASL-62555.

Sin embargo, el 802.1x ofrece al gestor de la red informado la posibilidad de diseñar e implementar una WLAN mucho más segura. De esta forma, en el panel

de ajustes de 802.1x, se precisa una dirección IP y un número de puerto para el servidor. El secreto es un recordatorio de consulta.

El valor hex PSK es una clave precompartida que se genera a partir de una paráfrasis. Para obtener el valor hex, se suelen emplear generadores de paráfrasis. Pueden encontrarse muchos de ellos en Internet. La cadena PSK funciona siguiendo un patrón similar. Se trata básicamente de un mecanismo de autenticación en el que los usuarios ofrecen algún tipo de credencial para verificar que se le debe permitir acceder a una red. Esto requiere una contraseña única introducida en cada nodo WLAN. Siempre que las contraseñas coincidan, un cliente podrá acceder a una WLAN. Ahora vamos a fijarnos en la configuración de WPA del ASL-26555.

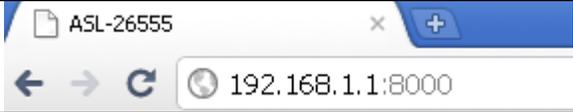
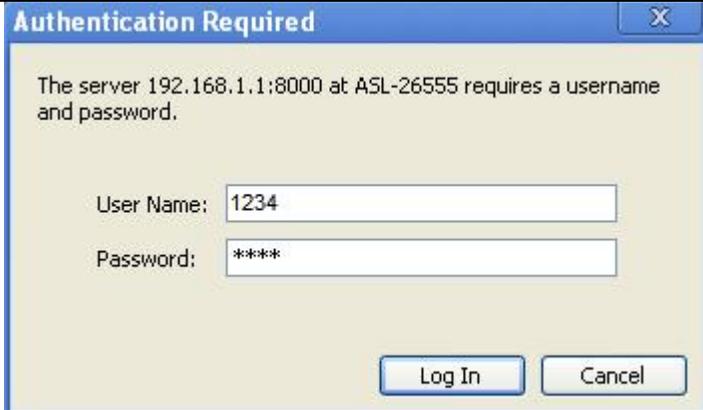
<p>WPA TYPE:</p>  <p>IMPORTANTE: La herramienta generadora de PIN en esta sección es específica del dispositivo ASL-26555.</p>	<p>Seleccione 802.1x. Seleccione la Server IP Address (Dirección IP del servidor) (se trata de una IP asignada al servidor RADIUS) Configure el número de Port (puerto) (se muestra un puerto por defecto) Secret (Secreto): Es un tipo de contraseña empleada para autenticar datos en el servidor Radius.</p> <p>En Wi-Fi Protected Setup (Configuración protegida Wi-Fi).</p> <p>Haga clic en la casilla Enable. Haga clic en Reset PIN to Default (Restaurar PIN al valor por defecto) para obtener un número de PIN o Haga clic en Generate New PIN (Generar nuevo PIN) para obtener un nuevo número de PIN. Haga clic en Add/Apply cuando haya terminado.</p> <p>En Wi-Fi Protected Status (Estado protegido Wi-Fi):</p> <p>El dispositivo muestra Enabled/Configured. Haga clic en Reset to Unconfigured</p>	
--	---	---

<p>WPA TYPE:</p> <p>Seleccione PSK HEX VALUE (Valor Hex PSK)</p> <p>En Hex Value</p> <p>Introduzca el Valor Hex que ha creado.</p> <p>En Wi-Fi Protected Setup (Configuración protegida Wi-Fi).</p> <p>Haga clic en el cuadro Enable. Haga clic en Reset PIN to Default para obtener un número de PIN o Haga clic en Generate New PIN para obtener un nuevo número de PIN. Haga clic en Add/Apply cuando haya terminado.</p> <p>En Wi-Fi Protected Status:</p> <p>El dispositivo muestra . Enabled/Configured Haga clic en Reset to Unconfigured</p>	
<p>WPA TYPE:</p> <p>Seleccione PSK String (Cadena PSK)</p> <p>En PSK string</p> <p>Introduzca la cadena que ha generado</p> <p>En Wi-Fi Protected Status.</p> <p>Haga clic en el cuadro Enable. Haga clic en Reset PIN to Default para obtener un número de PIN o Haga clic en Generate New PIN para obtener un nuevo número de PIN. Haga clic en Add/Apply cuando haya terminado.</p> <p>En Wi-Fi Protected Status:</p> <p>El dispositivo muestra . Enabled/Configured Haga clic en Reset to Unconfigured</p>	

Aspectos avanzados de la configuración inalámbrica

El ASL-26555 da al usuario la oportunidad de modificar otros aspectos del propio router para que pueda funcionar de manera independiente. Vamos a ver ahora cómo el ASL-26555 puede trabajar de forma estrecha con otros dispositivos de esta clase. Habilite esas funciones siguiendo estos pasos.

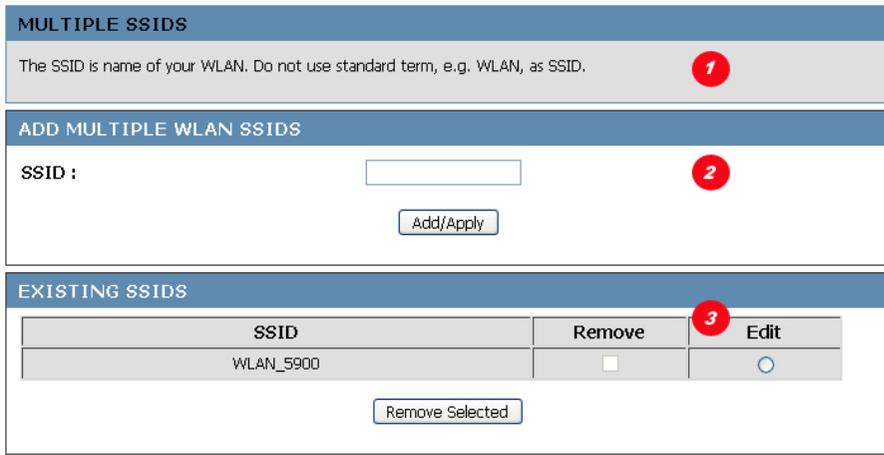
Reglas de acceso a la WLAN

Paso 1:	Abra el navegador y escriba la dirección IP por defecto del ASL-26555.	
Paso 2:	Escriba su Nombre de usuario y su Contraseña y haga clic en Log In .	
Paso 3:	Haga clic en Advanced y pase el ratón sobre Wireless Setup para ver la barra de navegación con pestañas.	
Paso 4:	Haga clic en WLAN Access Rules (Reglas de acceso a la WLAN) para editar o modificar las propiedades.	

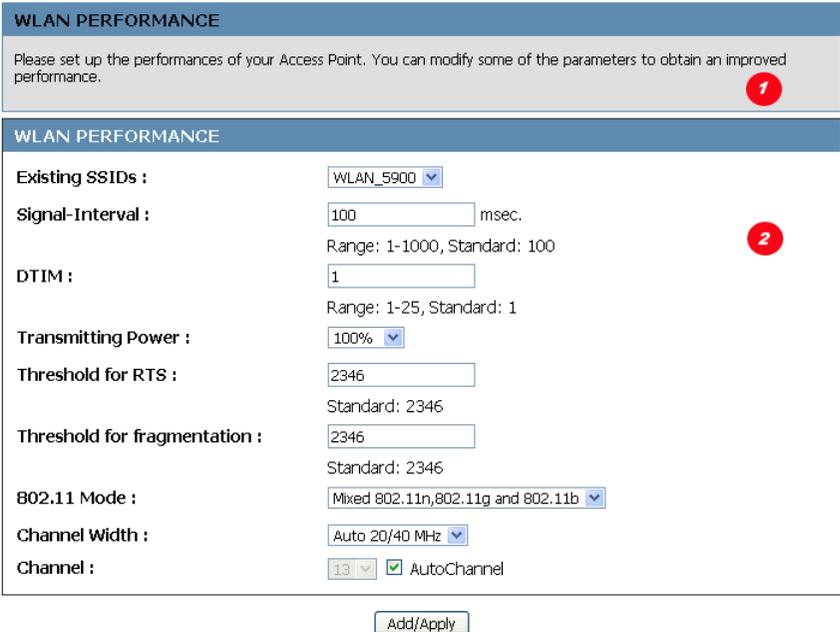
<p>Paso 5:</p>	<ol style="list-style-type: none"> 1. La primera ventana es una definición de las REGLAS DE ACCESO A LA WLAN. 2. La segunda ventana le permite editar las REGLAS DE ACCESO A LA WLAN. 3. La ventana tres le permite añadir direcciones MAC a la tabla de REGLAS DE ACCESO A LA WLAN. 	
<p>Paso 6:</p>	<p>Edite las políticas de acceso a la WLAN deshabilitando esta función, permitiendo a los ordenadores que aparecen en la lista acceder a la red inalámbrica o denegando a esos ordenadores acceder a la red inalámbrica. Haga clic en Add/Apply cuando haya terminado.</p>	
<p>Paso 7:</p>	<p>Se reiniciará la función inalámbrica.</p>	
<p>Paso 8:</p>	<p>Añada direcciones MAC a las reglas de acceso escribiendo las direcciones MAC y haga clic en Añadir y Aplicar.</p>	

Añadir SSID múltiples

<p>Paso 1:</p>	<p>Haga clic en Advanced y pase con el ratón sobre Wireless Setup para ver la barra de navegación de pestañas.</p>		
<p>Paso 2:</p>	<p>Haga clic en Multiple WLAN (SSID WLAN múltiples)</p>		

<p>Paso 3:</p>	<ol style="list-style-type: none"> 1. La primera ventana es una descripción de los SSID múltiples 2. La segunda ventana le permite añadir SSID 3. La tercera ventana le permite editar los SSID existentes 	
<p>Paso 4:</p>	<p>Escriba el SSID en el campo y haga clic en Add/Apply</p>	
<p>Paso 5:</p>	<p>Edite o elimine los SSID existentes marcando la casilla Remove (Eliminar) y haciendo clic en Removed Selected (Eliminar selección). La función de edición no está disponible en esta versión del programa.</p>	

WLAN PERFORMANCE (Rendimiento de la WLAN)

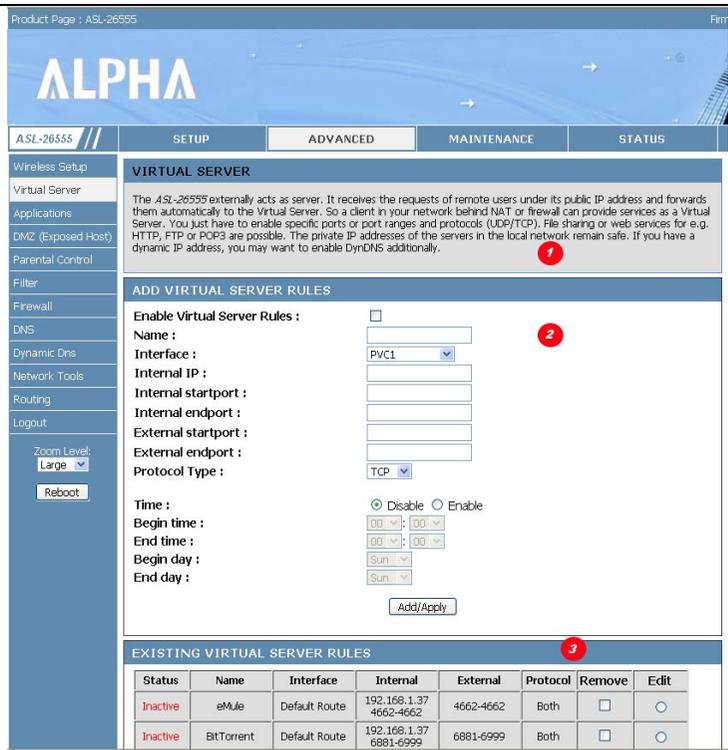
<p>Paso 1:</p>	<ol style="list-style-type: none"> 1. La primera ventana es una definición del Rendimiento de la WLAN. 2. La segunda ventana le permite editar los ajustes de rendimiento de la WLAN. 	
<p>Paso 2:</p>	<p>Seleccione un dispositivo SSID en la lista desplegable.</p>	<p>Existing SSIDs : WLAN_5900</p>
<p>Paso 3:</p>	<p>Escriba el número de veces que se transmite una señal. Se da un ejemplo de un rango, donde se sugiere que 100 sea el estándar.</p>	<p>Signal-Interval : 100 msec. Range: 1-1000, Standard: 100</p>
<p>Paso 4:</p>	<p>La entrada Mensaje de indicación de tráfico de entrega (DTIM) está configurada en 1, el rango recomendado.</p>	<p>DTIM : 1 Range: 1-25, Standard: 1</p>
<p>Paso 5:</p>	<p>En la lista desplegable, seleccione la Potencia de transmisión.</p>	<p>100% 100% 50% 25% 12.5%</p>
<p>Paso 6:</p>	<p>Siga la recomendación por defecto para el umbral RTS.</p>	<p>Threshold for RTS : 2346 Standard: 2346</p>

Paso 7:	Escriba la fragmentación de umbral sugerida.	Threshold for fragmentation : <input type="text" value="2346"/> Standard: 2346
Paso 8:	Seleccione el tipo de modo inalámbrico con el que desea que opere el ASL-26555, siendo 802.11n el más fuerte.	Mixed 802.11n,802.11g and 802.11b ▼ 802.11b Only 802.11g Only Mixed 802.11g and 820.11b 802.11n Only Mixed 802.11g and 820.11n Mixed 802.11n,802.11g and 802.11b
Paso 9:	Seleccione la Anchura de canal en el menú desplegable.	Auto 20/40 MHz ▼ 20 MHz Auto 20/40 MHz
Paso 10:	Por último, seleccione Canal auto para permitir al dispositivo elegir la mejor operabilidad o seleccione un elemento de la lista desplegable. Si selecciona auto significa que el ASL-26555 elegirá el canal con el menor número de dispositivos conectados.	13 ▼ 1 2 3 4 5 6 7 8 9 10 11 12 13
Paso 11:	Haga clic en Add/Apply cuando haya terminado.	

Capítulo 14: Configuración del servidor virtual

Descripción general

El ASL-26555 actúa como un servidor virtual con los dispositivos conectados localmente a él. El ASL-62555 utiliza mapeo de puertos para habilitar funciones como FTP, POP3 y varios paquetes de software de juegos y torrents. Esto ofrece una mayor flexibilidad y funcionalidad. Vamos a ver algunas de sus funciones. Su router permite a todos sus ordenadores compartir una única dirección IP "real" en Internet. También le protege impidiendo que la entrada de conexiones desde el exterior pueda dañar sus ordenadores. Pero para aceptar conexiones de servidores web o BitTorrent tendrá que abrir un agujero en el cortafuegos de su router para que pase el tráfico a través de un ordenador en los puertos elegidos.

<p>La interfaz</p> <ol style="list-style-type: none"> 1. Explicación de lo que es un servidor virtual 2. Un lugar en el que añadir reglas de servidor virtual. 3. Reglas de servidor virtual existentes <p> IMPORTANTE: El tráfico TCP (protocolo de control de transmisión) es el tipo de tráfico más habitual. Es todo lo que necesita para un sitio web. También se utiliza UDP (protocolo de datagramas de usuario) en algunos tipos de programas BitTorrent, por lo que debe habilitar tanto TCP como UDP para BitTorrent.</p>		
<p>Paso 1:</p>	<p>Haga clic en Habilitar reglas de servidor virtual</p>	<p>Enable Virtual Server Rules : <input type="checkbox"/></p>

Paso 2:	Seleccione un nombre para el servidor virtual	Name : <input type="text"/>
Paso 3:	Seleccione una interfaz en la lista desplegable.  IMPORTANTE: Si sólo ha configurado un PVC, sólo le dará esa opción. Sin embargo, también ofrece la ruta por defecto.	Interface : <input type="text" value="PVC1"/>
Paso 4:	Escriba una IP interna. Esa IP suele ser la IP configurada por defecto en su router	Internal IP : <input type="text"/>
Paso 5:	Escriba un número de puerto inicial y puerto final internos.  IMPORTANTE: Para obtener una lista completa de los números de puerto y sus usos de software correspondientes, busque en la Wikipedia o Google	Internal startport : <input type="text"/> Internal endport : <input type="text"/>
Paso 6:	Escriba un puerto inicial y un puerto final externos.  IMPORTANTE: Los números de puerto internos deben corresponderse con los puertos externos	External startport : <input type="text"/> External endport : <input type="text"/>
Paso 7:	En la lista desplegable, seleccione TCP , UDP o Both (Ambos) .	Protocol Type : <input type="text" value="TCP"/>
Paso 8:	Haga clic en Enable para crear un marco temporal para la activación del servidor virtual	Time : <input checked="" type="radio"/> Disable <input type="radio"/> Enable

<p>Paso 9:</p>	<p>Seleccione la hora (inicio/fin) y el día (inicio/fin) para activar la duración del servidor virtual. Haga clic en Add/Apply.</p>	<p>Begin time : 00 : 00</p> <p>End time : 00 : 00</p> <p>Begin day : Sun</p> <p>End day : Sun</p> <p style="text-align: right;">Add/Apply</p>																																																																																																																																																								
<p>Paso 10:</p>	<p>La pantalla final de la sección dedicada al servidor virtual se ocupa de las Existing Virtual Server Rules (Reglas de servidor virtual existentes). Cuando haya añadido dispositivos al router, la información sobre los mismos aparecerá en esta área.</p> <p>Para eliminar una regla, sólo tiene que hacer clic en la casilla de verificación Remove (Eliminar) y hacer clic en Removed selected (Eliminar selección) en la parte inferior de la página.</p> <p>La función Edit (Editar) aparece deshabilitada en el momento de esta publicación.</p>	<p>EXISTING VIRTUAL SERVER RULES</p> <table border="1"> <thead> <tr> <th>Status</th> <th>Name</th> <th>Interface</th> <th>Internal</th> <th>External</th> <th>Protocol</th> <th>Remove</th> <th>Edit</th> </tr> </thead> <tbody> <tr> <td>Inactive</td> <td>eMule</td> <td>Default Route</td> <td>192.168.1.37 4662-4662</td> <td>4662-4662</td> <td>Both</td> <td><input type="checkbox"/></td> <td><input type="radio"/></td> </tr> <tr> <td>Inactive</td> <td>BitTorrent</td> <td>Default Route</td> <td>192.168.1.37 6881-6999</td> <td>6881-6999</td> <td>Both</td> <td><input type="checkbox"/></td> <td><input type="radio"/></td> </tr> <tr> <td>Inactive</td> <td>Xbox Live</td> <td>Default Route</td> <td>192.168.1.34 53-53</td> <td>53-53</td> <td>Both</td> <td><input type="checkbox"/></td> <td><input type="radio"/></td> </tr> <tr> <td>Inactive</td> <td>Xbox Live</td> <td>Default Route</td> <td>192.168.1.34 88-88</td> <td>88-88</td> <td>Both</td> <td><input type="checkbox"/></td> <td><input type="radio"/></td> </tr> <tr> <td>Inactive</td> <td>Xbox Live</td> <td>Default Route</td> <td>192.168.1.34 3074-3074</td> <td>3074-3074</td> <td>Both</td> <td><input type="checkbox"/></td> <td><input type="radio"/></td> </tr> <tr> <td>Inactive</td> <td>Transmission</td> <td>Default Route</td> <td>192.168.1.34 51413-51413</td> <td>51413-51413</td> <td>Both</td> <td><input type="checkbox"/></td> <td><input type="radio"/></td> </tr> <tr> <td>Inactive</td> <td>PlatStation Network</td> <td>Default Route</td> <td>192.168.1.38 80-80</td> <td>80-80</td> <td>TCP</td> <td><input type="checkbox"/></td> <td><input type="radio"/></td> </tr> <tr> <td>Inactive</td> <td>PlatStation Network</td> <td>Default Route</td> <td>192.168.1.38 443-443</td> <td>443-443</td> <td>TCP</td> <td><input type="checkbox"/></td> <td><input type="radio"/></td> </tr> <tr> <td>Inactive</td> <td>PlatStation Network</td> <td>Default Route</td> <td>192.168.1.38 5223-5223</td> <td>5223-5223</td> <td>TCP</td> <td><input type="checkbox"/></td> <td><input type="radio"/></td> </tr> <tr> <td>Inactive</td> <td>PlatStation Network</td> <td>Default Route</td> <td>192.168.1.38 3478-3479</td> <td>3478-3479</td> <td>UDP</td> <td><input type="checkbox"/></td> <td><input type="radio"/></td> </tr> <tr> <td>Inactive</td> <td>PlatStation Network</td> <td>Default Route</td> <td>192.168.1.38 3658-3658</td> <td>3658-3658</td> <td>UDP</td> <td><input type="checkbox"/></td> <td><input type="radio"/></td> </tr> <tr> <td>Inactive</td> <td>PlayStation Remote Play</td> <td>Default Route</td> <td>192.168.1.38 9293-9293</td> <td>9293-9293</td> <td>Both</td> <td><input type="checkbox"/></td> <td><input type="radio"/></td> </tr> <tr> <td>Inactive</td> <td>World of Warcraft</td> <td>Default Route</td> <td>192.168.1.37 3742-3742</td> <td>3742-3742</td> <td>TCP</td> <td><input type="checkbox"/></td> <td><input type="radio"/></td> </tr> <tr> <td>Inactive</td> <td>World of Warcraft</td> <td>Default Route</td> <td>192.168.1.37 6112-6112</td> <td>6112-6112</td> <td>TCP</td> <td><input type="checkbox"/></td> <td><input type="radio"/></td> </tr> <tr> <td>Inactive</td> <td>MSN Gaming Zone</td> <td>Default Route</td> <td>192.168.1.34 6667-6667</td> <td>6667-6667</td> <td>TCP</td> <td><input type="checkbox"/></td> <td><input type="radio"/></td> </tr> <tr> <td>Inactive</td> <td>MSN Gaming Zone</td> <td>Default Route</td> <td>192.168.1.34 28800-29000</td> <td>28800-29000</td> <td>UDP</td> <td><input type="checkbox"/></td> <td><input type="radio"/></td> </tr> <tr> <td>Inactive</td> <td>MSN Gaming Zone</td> <td>Default Route</td> <td>192.168.1.34 2300-2400</td> <td>2300-2400</td> <td>Both</td> <td><input type="checkbox"/></td> <td><input type="radio"/></td> </tr> <tr> <td>Inactive</td> <td>MSN Gaming Zone</td> <td>Default Route</td> <td>192.168.1.34 47624-47624</td> <td>47624-47624</td> <td>TCP</td> <td><input type="checkbox"/></td> <td><input type="radio"/></td> </tr> </tbody> </table> <p style="text-align: center;">Remove Selected</p>	Status	Name	Interface	Internal	External	Protocol	Remove	Edit	Inactive	eMule	Default Route	192.168.1.37 4662-4662	4662-4662	Both	<input type="checkbox"/>	<input type="radio"/>	Inactive	BitTorrent	Default Route	192.168.1.37 6881-6999	6881-6999	Both	<input type="checkbox"/>	<input type="radio"/>	Inactive	Xbox Live	Default Route	192.168.1.34 53-53	53-53	Both	<input type="checkbox"/>	<input type="radio"/>	Inactive	Xbox Live	Default Route	192.168.1.34 88-88	88-88	Both	<input type="checkbox"/>	<input type="radio"/>	Inactive	Xbox Live	Default Route	192.168.1.34 3074-3074	3074-3074	Both	<input type="checkbox"/>	<input type="radio"/>	Inactive	Transmission	Default Route	192.168.1.34 51413-51413	51413-51413	Both	<input type="checkbox"/>	<input type="radio"/>	Inactive	PlatStation Network	Default Route	192.168.1.38 80-80	80-80	TCP	<input type="checkbox"/>	<input type="radio"/>	Inactive	PlatStation Network	Default Route	192.168.1.38 443-443	443-443	TCP	<input type="checkbox"/>	<input type="radio"/>	Inactive	PlatStation Network	Default Route	192.168.1.38 5223-5223	5223-5223	TCP	<input type="checkbox"/>	<input type="radio"/>	Inactive	PlatStation Network	Default Route	192.168.1.38 3478-3479	3478-3479	UDP	<input type="checkbox"/>	<input type="radio"/>	Inactive	PlatStation Network	Default Route	192.168.1.38 3658-3658	3658-3658	UDP	<input type="checkbox"/>	<input type="radio"/>	Inactive	PlayStation Remote Play	Default Route	192.168.1.38 9293-9293	9293-9293	Both	<input type="checkbox"/>	<input type="radio"/>	Inactive	World of Warcraft	Default Route	192.168.1.37 3742-3742	3742-3742	TCP	<input type="checkbox"/>	<input type="radio"/>	Inactive	World of Warcraft	Default Route	192.168.1.37 6112-6112	6112-6112	TCP	<input type="checkbox"/>	<input type="radio"/>	Inactive	MSN Gaming Zone	Default Route	192.168.1.34 6667-6667	6667-6667	TCP	<input type="checkbox"/>	<input type="radio"/>	Inactive	MSN Gaming Zone	Default Route	192.168.1.34 28800-29000	28800-29000	UDP	<input type="checkbox"/>	<input type="radio"/>	Inactive	MSN Gaming Zone	Default Route	192.168.1.34 2300-2400	2300-2400	Both	<input type="checkbox"/>	<input type="radio"/>	Inactive	MSN Gaming Zone	Default Route	192.168.1.34 47624-47624	47624-47624	TCP	<input type="checkbox"/>	<input type="radio"/>
Status	Name	Interface	Internal	External	Protocol	Remove	Edit																																																																																																																																																			
Inactive	eMule	Default Route	192.168.1.37 4662-4662	4662-4662	Both	<input type="checkbox"/>	<input type="radio"/>																																																																																																																																																			
Inactive	BitTorrent	Default Route	192.168.1.37 6881-6999	6881-6999	Both	<input type="checkbox"/>	<input type="radio"/>																																																																																																																																																			
Inactive	Xbox Live	Default Route	192.168.1.34 53-53	53-53	Both	<input type="checkbox"/>	<input type="radio"/>																																																																																																																																																			
Inactive	Xbox Live	Default Route	192.168.1.34 88-88	88-88	Both	<input type="checkbox"/>	<input type="radio"/>																																																																																																																																																			
Inactive	Xbox Live	Default Route	192.168.1.34 3074-3074	3074-3074	Both	<input type="checkbox"/>	<input type="radio"/>																																																																																																																																																			
Inactive	Transmission	Default Route	192.168.1.34 51413-51413	51413-51413	Both	<input type="checkbox"/>	<input type="radio"/>																																																																																																																																																			
Inactive	PlatStation Network	Default Route	192.168.1.38 80-80	80-80	TCP	<input type="checkbox"/>	<input type="radio"/>																																																																																																																																																			
Inactive	PlatStation Network	Default Route	192.168.1.38 443-443	443-443	TCP	<input type="checkbox"/>	<input type="radio"/>																																																																																																																																																			
Inactive	PlatStation Network	Default Route	192.168.1.38 5223-5223	5223-5223	TCP	<input type="checkbox"/>	<input type="radio"/>																																																																																																																																																			
Inactive	PlatStation Network	Default Route	192.168.1.38 3478-3479	3478-3479	UDP	<input type="checkbox"/>	<input type="radio"/>																																																																																																																																																			
Inactive	PlatStation Network	Default Route	192.168.1.38 3658-3658	3658-3658	UDP	<input type="checkbox"/>	<input type="radio"/>																																																																																																																																																			
Inactive	PlayStation Remote Play	Default Route	192.168.1.38 9293-9293	9293-9293	Both	<input type="checkbox"/>	<input type="radio"/>																																																																																																																																																			
Inactive	World of Warcraft	Default Route	192.168.1.37 3742-3742	3742-3742	TCP	<input type="checkbox"/>	<input type="radio"/>																																																																																																																																																			
Inactive	World of Warcraft	Default Route	192.168.1.37 6112-6112	6112-6112	TCP	<input type="checkbox"/>	<input type="radio"/>																																																																																																																																																			
Inactive	MSN Gaming Zone	Default Route	192.168.1.34 6667-6667	6667-6667	TCP	<input type="checkbox"/>	<input type="radio"/>																																																																																																																																																			
Inactive	MSN Gaming Zone	Default Route	192.168.1.34 28800-29000	28800-29000	UDP	<input type="checkbox"/>	<input type="radio"/>																																																																																																																																																			
Inactive	MSN Gaming Zone	Default Route	192.168.1.34 2300-2400	2300-2400	Both	<input type="checkbox"/>	<input type="radio"/>																																																																																																																																																			
Inactive	MSN Gaming Zone	Default Route	192.168.1.34 47624-47624	47624-47624	TCP	<input type="checkbox"/>	<input type="radio"/>																																																																																																																																																			

Capítulo 15: Configuración de aplicaciones especiales

Descripción general

Las aplicaciones especiales del ASL-26555 se refieren a programas de Internet que necesitan un acceso especial a la red. Dicho de otra forma, necesitan traspasar el cortafuegos y tener un acceso especial al router. Esta sección presenta el software, el puerto y la aplicación para hacerlo. Éstas son las herramientas que necesita para ello.

- Paso 1:**
1. La primera ventana es una definición de la **Aplicación especial**
 2. La ventana dos le permite configurar la aplicación.
 3. La ventana tres le permite ver las aplicaciones existentes y eliminarlas.

Product Page : ASL-26555 Firmware Version : v1.1.0.8_PE

ALPHA

ASL-26555 // SETUP ADVANCED MAINTENANCE STATUS HELP

Wireless Setup
Virtual Server
Applications
DMZ (Exposed Host)
Parental Control
Filter
Firewall
DNS
Dynamic Dns
Network Tools
Routing
Logout
Zoom Level: Small Reboot

SPECIAL APPLICATION 1

The Application is used to open single or multiple ports in your firewall when the router senses data sent to the Internet on a outgoing "Trigger" port or port range. Applications rules apply to all computers on your internal network.

SPECIAL APPLICATION 2

Enable Application : Disabled Enabled

Name :

Trigger Port Start :

Trigger Port End :

Trigger Traffic Protocol Type :

Trigger Source IP:

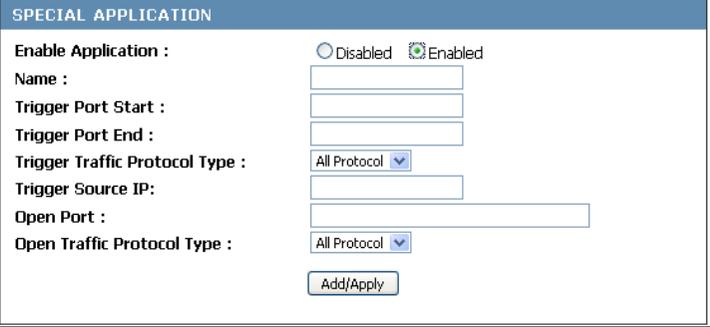
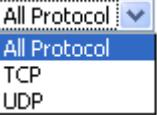
Open Port :

Open Traffic Protocol Type :

EXISTING APPLICATION 3

Status	Name	Trigger Source IP/port	Trigger Traffic Protocol Type	Open Port	Open Traffic Protocol Type	Remove	Edit
Inactive	Battle.net	Any/6112~	All Protocol	6112	All Protocol	<input type="checkbox"/>	<input type="checkbox"/>
Inactive	Dialpad	Any/7175~	All Protocol	51200-51201, 51210	All Protocol	<input type="checkbox"/>	<input type="checkbox"/>
Inactive	ICU II	Any/2019~	All Protocol	2000-2030, 2050-2051, 2069-2085, 2010-3030	All Protocol	<input type="checkbox"/>	<input type="checkbox"/>
Inactive	MSN Gaming Zone	Any/47624~	All Protocol	2300-2400, 28800-29000	All Protocol	<input type="checkbox"/>	<input type="checkbox"/>
Inactive	PC-to-Phone	Any/12053~	All Protocol	12120, 12122, 24150-24220	All Protocol	<input type="checkbox"/>	<input type="checkbox"/>
Inactive	Quick Time 4	Any/854~	All Protocol	6970-6999	All Protocol	<input type="checkbox"/>	<input type="checkbox"/>
Active	XBOX360-1	Any/3074~	All Protocol	3074	All Protocol	<input type="checkbox"/>	<input type="checkbox"/>
Active	XBOX360-2	Any/88~	UDP	88	UDP	<input type="checkbox"/>	<input type="checkbox"/>

Helpful Hints...
The Application is used to open single or multiple ports in your firewall, when the router senses data sent to the Internet on a outgoing "Trigger" port or port range. Applications rules apply to all computers on your internal network.

<p>Paso 2:</p>	<p>En SPECIAL APPLICATION (Aplicación especial), haga clic en Enable</p>	
<p>Paso 3:</p>	<p>Escriba el nombre de la aplicación (por ejemplo: dialpad)</p>	<p>Name : <input type="text"/></p>
<p>Paso 4:</p>	<p>En Inicio del puerto de activación, escriba</p>	<p>Trigger Port Start : <input type="text"/></p>
<p>Paso 5:</p>	<p>En Final del puerto de activación, escriba el número de puerto</p>	<p>Trigger Port End : <input type="text"/></p>
<p>Paso 6:</p>	<p>Seleccione Todos los protocolos en Tipo de protocolo de tráfico de activación</p>	
<p>Paso 7:</p>	<p>En IP del puerto de activación, escriba cualquiera</p>	<p>Trigger Source IP: <input type="text"/></p>
<p>Paso 8:</p>	<p>En Puerto abierto, escriba el número de puerto</p>	<p>Open Port : <input type="text"/></p>
<p>Paso 9:</p>	<p>En Tipo de protocolo de tráfico abierto, seleccione Todos los protocolos en el menú desplegable</p>	
<p>Paso 10</p>	<p>Haga clic en Add/Apply</p>	<p><input type="button" value="Add/Apply"/></p>

Paso 11: Para ver o editar las aplicaciones existentes, muévase por **EXISTING APPLICATION (Aplicaciones existentes)** y haga clic en los botones **Remove (Eliminar)** o **Edit (Editar)**

Tenga en cuenta que las aplicaciones inactivas aparecen en **rojo** y que las aplicaciones activas se señalan en **azul**.

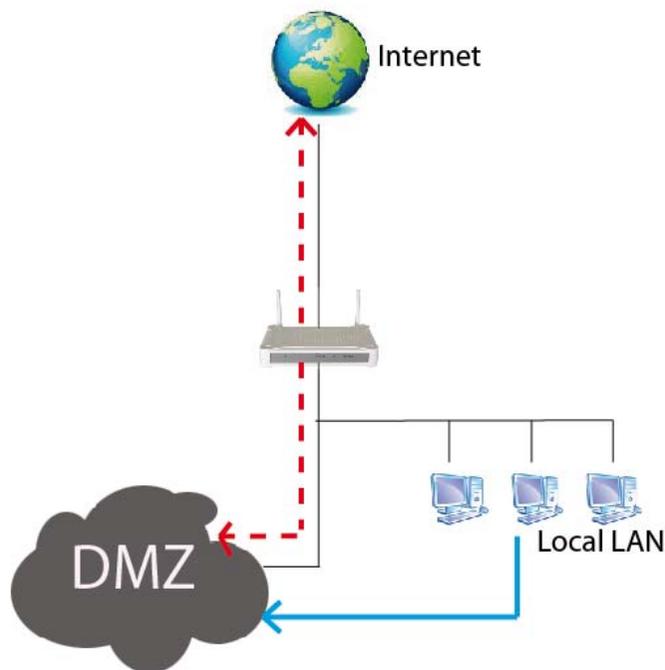
Para eliminar una aplicación marque su casilla de verificación **Remove (Eliminar)** y haga clic en **Remove Selected (Eliminar selección)**.

EXISTING APPLICATION							
Status	Name	Trigger Source IP/port	Trigger Traffic Protocol Type	Open Port	Open Traffic Protocol Type	Remove	Edit
Inactive	Battle.net	Any/6112~	All Protocol	6112	All Protocol	<input type="checkbox"/>	<input type="radio"/>
Inactive	Dialpad	Any/7175~	All Protocol	51200-51201, 51210	All Protocol	<input type="checkbox"/>	<input type="radio"/>
Inactive	ICU II	Any/2019~	All Protocol	2000-2038, 2050-2051, 2069, 2085, 3010-3030	All Protocol	<input type="checkbox"/>	<input type="radio"/>
Inactive	MSN Gaming Zone	Any/47624~	All Protocol	2300-2400, 28800-29000	All Protocol	<input type="checkbox"/>	<input type="radio"/>
Inactive	PC-to-Phone	Any/12053~	All Protocol	12120, 12122, 24150-24220	All Protocol	<input type="checkbox"/>	<input type="radio"/>
Inactive	Quick Time 4	Any/554~	All Protocol	6970-6999	All Protocol	<input type="checkbox"/>	<input type="radio"/>
Active	XBOX360-1	Any/3074~	All Protocol	3074	All Protocol	<input type="checkbox"/>	<input type="radio"/>
Active	XBOX360-2	Any/88~	UDP	88	UDP	<input type="checkbox"/>	<input type="radio"/>

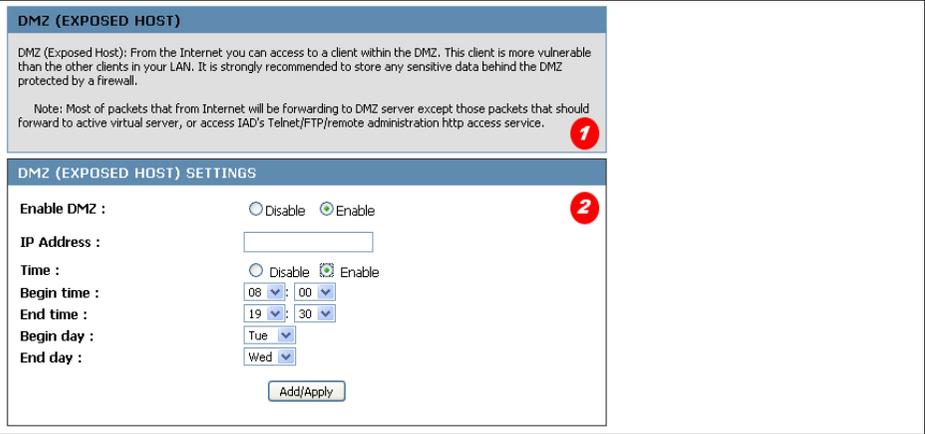
Capítulo 16: Configuración de la DMZ

Descripción general

La DMZ es una zona especial creada dentro de la subred para impedir que los datos lleguen a clientes sensibles de su red. Actúa como escudo protector con respecto a la red ordinaria. Los datos pueden transferirse de Internet al DMZ y los clientes que operen dentro de su LAN pueden conectarse a la DMZ. Sin embargo, la DMZ no puede conectarse a la LAN interna. Sigue una ilustración más clara de lo que ocurre.



La línea gris de la ilustración muestra la topología normal de una LAN. La línea punteada roja ilustra la comunicación entre la zona DMZ e Internet. Por su parte, la línea azul sólo indica el tráfico entre la DMZ y la LAN local.

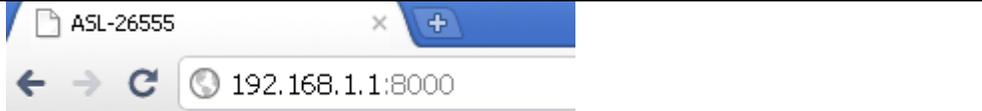
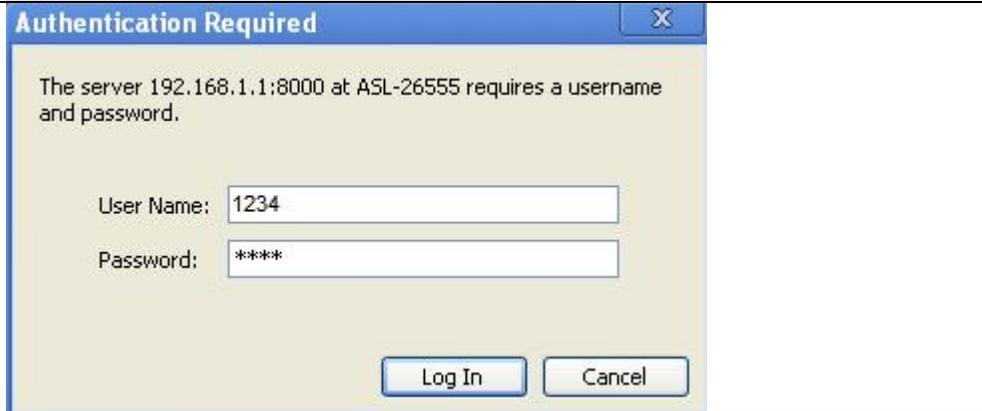
<p>Paso 1:</p>	<p>Abra el navegador y escriba la dirección IP por defecto del ASL-26555.</p>	
<p>Paso 2:</p>	<p>Escriba su Nombre de usuario y su Contraseña y haga clic en Log In.</p>	
<p>Paso 3:</p>	<p>Haga clic en ADVANCED, DMZ (EXPOSED HOST).</p>	
<p>Paso 4:</p> <p>La DMZ tiene dos ventanas:</p> <ol style="list-style-type: none"> 1. La primera ventana es la descripción 2. La segunda ventana es la zona de configuración 		
<p>Paso 5:</p>	<p>En Enable DMZ, haga clic en Enable</p>	
<p>Paso 6:</p>	<p>Escriba la Dirección IP del servidor DMZ</p>	

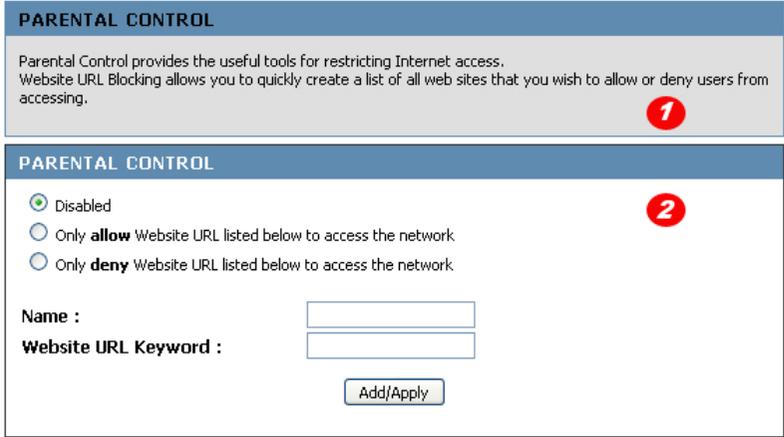
Paso 7:	En Hora , haga clic en Enable y configure la hora y la fecha para activar el servidor DMZ (zona)	<p>Time : <input type="radio"/> Disable <input checked="" type="radio"/> Enable</p> <p>Begin time : 08 : 00</p> <p>End time : 19 : 30</p> <p>Begin day : Tue</p> <p>End day : Wed</p>
Paso 8:	Haga clic en Add/Apply	<input type="button" value="Add/Apply"/>

Capítulo 17: Configuración del control parental

Descripción general

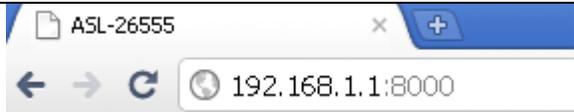
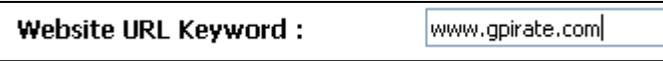
El control parental permite a los usuarios restringir el derecho de acceso a determinados sitios desde el ASL-26555. Los administradores pueden denegar el acceso a salas de chat, redes sociales o incluso sitios ofensivos utilizando el control parental. Siga estos sencillos pasos para deshabilitar esta función y dar a los usuarios total libertad o crear una lista de sitios que considera impropios para su red.

Paso 1:	Abra el navegador y escriba la dirección IP por defecto del ASL-26555.	
Paso 2:	Escriba su Nombre de usuario y su Contraseña y haga clic en Log In .	
Paso 3:	Haga clic en Advanced, Parental Control (Control parental) .	

<p>Paso 4: Control parental tiene dos ventanas:</p> <ol style="list-style-type: none"> 1. La primera ventana es la descripción 2. La segunda ventana es la zona de configuración 																		
<p>Paso 5: Haga clic en Disabled si no desea hacer ningún cambio</p>																		
<p>Paso 6: Haga clic en Permitir acceder a la red sólo a las URL de la lista.</p>																		
<p>Paso 7: Escriba el Nombre del sitio al que desea permitir el acceso. En este ejemplo, hemos usado Sony como sitio permitido.</p>																		
<p>Paso 8: Escriba la dirección web en Palabra clave de la URL</p>																		
<p>Paso 9: Haga clic en Add/Apply</p>																		
<p>Paso 10: Debería aparecer una lista con las URL permitidas.</p>		 <table border="1" data-bbox="1167 1070 1921 1217"> <thead> <tr> <th>Name</th> <th>Website URL Keyword</th> <th>Remove</th> <th>Edit</th> </tr> </thead> <tbody> <tr> <td>playboy</td> <td>www.playboy.com</td> <td><input type="checkbox"/></td> <td><input type="radio"/></td> </tr> <tr> <td>sony</td> <td>www.sony.com</td> <td><input type="checkbox"/></td> <td><input type="radio"/></td> </tr> <tr> <td>torrent</td> <td>www.gpirate.com</td> <td><input type="checkbox"/></td> <td><input type="radio"/></td> </tr> </tbody> </table>	Name	Website URL Keyword	Remove	Edit	playboy	www.playboy.com	<input type="checkbox"/>	<input type="radio"/>	sony	www.sony.com	<input type="checkbox"/>	<input type="radio"/>	torrent	www.gpirate.com	<input type="checkbox"/>	<input type="radio"/>
Name	Website URL Keyword	Remove	Edit															
playboy	www.playboy.com	<input type="checkbox"/>	<input type="radio"/>															
sony	www.sony.com	<input type="checkbox"/>	<input type="radio"/>															
torrent	www.gpirate.com	<input type="checkbox"/>	<input type="radio"/>															

Control parental – Bloquear un sitio

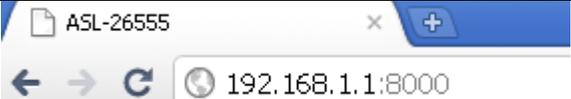
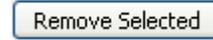
El ASL-26555 puede bloquear sitios no deseables o sitios de empresas consideradas como desfavorables para el entorno de trabajo. Siga estos pasos para denegar el acceso a un sitio.

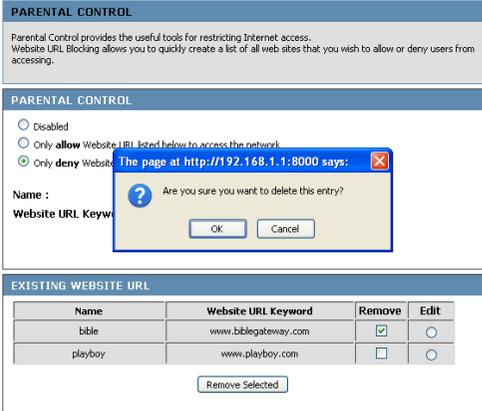
Paso 1:	Abra el navegador y escriba la dirección IP por defecto del ASL-26555.	
Paso 2:	Escriba su Nombre de usuario y su Contraseña y haga clic en Log In .	
Paso 3:	Haga clic en Advanced, Parental Control	
Paso 6:	Haga clic en Denegar el acceso a la red sólo a las URL de la lista .	
Paso 7:	Escriba el Nombre del sitio al que desea denegar el acceso. En este ejemplo, hemos usado gpirate como sitio no permitido .	
Paso 8:	Escriba la dirección web en Palabra clave de la URL	
Paso 9:	Haga clic en Add/Apply	

<p>Paso 10: Debería aparecer una lista con las URL bloqueadas.</p>		
---	--	---

Control parental – Eliminación de un sitio

Elimina un sitio de la lista de sitios permitidos o no permitido es muy sencillo. Siga estos pasos:

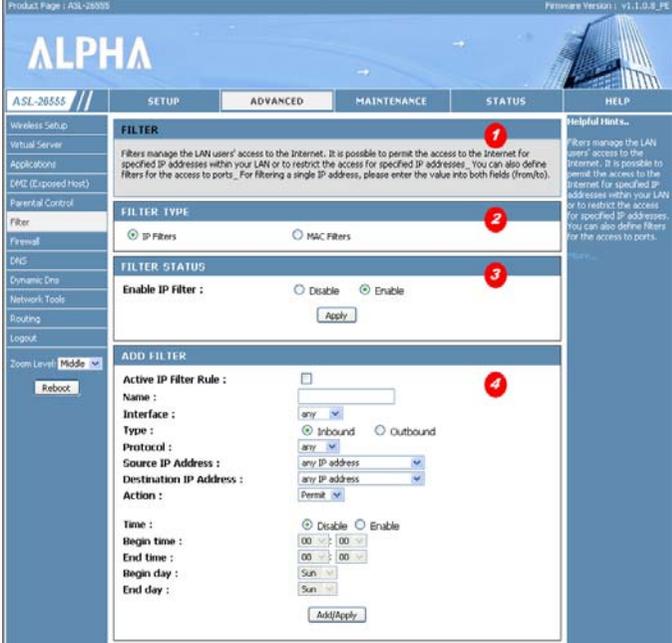
<p>Paso 1: Abra el navegador y escriba la dirección IP por defecto del ASL-26555.</p>		
<p>Paso 2: Escriba su Nombre de usuario y su Contraseña y haga clic en Log In.</p>		
<p>Paso 3: Haga clic en Advanced, Parental Control.</p>		
<p>Paso 4: Marque la casilla de verificación Remove (Eliminar) en la ventana URL existentes.</p>		
<p>Paso 5: Haga clic en Remove Selected (Eliminar selección)</p>		

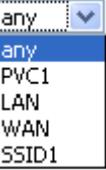
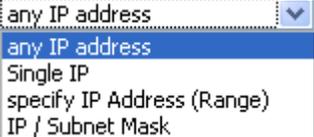
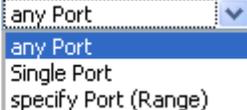
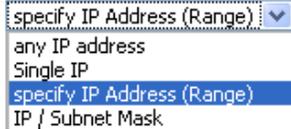
<p>Paso 6:</p>	<p>Aparecerá una ventana pidiéndole que verifique la decisión.</p>	
<p>Paso 7:</p>	<p>Haga clic en OK para verificarla.</p>	
<p>Paso 8:</p>	<p>La lista se actualizará para mostrar las nuevas URL existentes</p>	

Capítulo 18: Configuración de la función de filtrado

Descripción general

Los filtros gestionan el acceso a Internet de los usuarios de la LAN. Cuando un administrador de sistemas tiene varios nodos (PC) en la red y concede privilegios especiales a cada usuario, esos nodos también necesitan privilegios específicos al acceder a la red. Esos PC tienen cada uno una dirección IP y una dirección MAC. La forma de controlar el acceso a Internet de esos nodos es emplear filtros. Los filtros pueden controlar también los privilegios de los puertos. La mayoría de los paquetes de software necesitan puertos para canalizar esta función. Los filtros pueden permitir acceder a esos puertos y limitar el uso de puertos concretos por parte de los usuarios. Vamos a ver ahora cómo configurar los filtros.

<p>Paso 1:</p> <p>La interfaz Filter (Filtro) tiene cuatro ventanas:</p> <ol style="list-style-type: none"> 1. La primera ventana es la descripción 2. La segunda ventana selecciona el tipo de filtro 3. La tercera ventana selecciona el estado del filtro 4. La cuarta ventana le permite configurar las opciones de filtrado <p> IMPORTANTE: La sección principal es la cuarta ventana, la ventana de configuración. Contiene muchas opciones para elegir una vez que ha seleccionado su tipo de filtro y lo ha habilitado.</p>		
<p>Paso 2:</p>	<p>En FILTER TYPE (Tipo de filtro), seleccione IP FILTERS (Filtros IP)</p>	

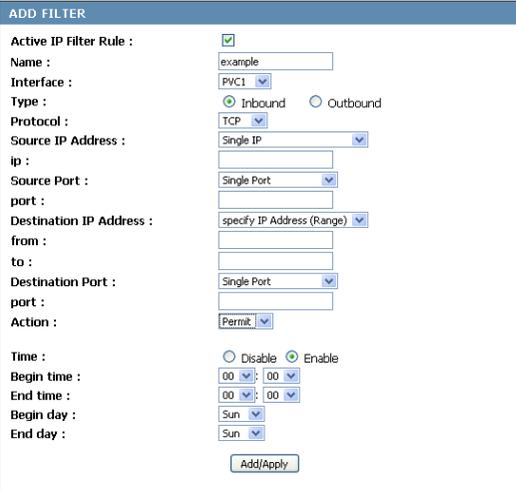
Paso 3:	En FILTER STATUS (Estado del filtro) , haga clic en Habilitar filtro IP	
Paso 4:	En Añadir filtro , haga clic en Regla de filtro IP activa	Active IP Filter Rule : <input type="checkbox"/>
Paso 5:	Escriba un nombre par el filtro	Name : <input type="text"/>
Paso 6:	Seleccione el tipo de interfaz en la lista desplegable. Ese filtro será específico del tipo de interfaz de red que desee emplear. La interfaz puede ser PVC1 (el servidor virtual que ha creado antes), LAN , WAN o SSID	
Paso 7:	Seleccione si el filtro será de bajada o de subida .	Type : <input checked="" type="radio"/> Inbound <input type="radio"/> Outbound
Paso 8:	Seleccione un protocolo en la lista desplegable. Aquí puede seleccionar cualquiera (esta opción deja elegir al programa) o ser más específico y seleccionar entre estas tres opciones: TCP , UDP o ICMP	
Paso 9:	Seleccione la Dirección IP de origen en la lista desplegable. Puede ser cualquier dirección IP , una IP individual , un rango de direcciones IP o una IP con su máscara de subred . Cuando realice su selección, la pantalla cambiará automáticamente para adaptarse a las elecciones que haya hecho. Vea los Escenarios que siguen.	
Paso 10:	Seleccione un origen de Puerto . Esta selección le permitirá elegir entre cualquier Puerto , un Puerto individual o especificar un rango de Puertos .	Source Port : 
Paso 11:	Seleccione la Dirección IP de destino . Aquí también accederá a una lista desplegable: cualquier dirección IP , dirección IP individual , especificar direcciones IP (rango) o IP con su máscara de subred .	Destination IP Address : 
Paso 12:	Seleccione el Puerto de destino en la lista desplegable. Existen tres opciones: cualquier puerto , puerto individual , especificar puertos (rango) . Seleccione la opción que mejor se adapte a sus necesidades.	Destination Port : 

<p>Paso 13:</p>	<p>Seleccione una Acción. Esa acción puede ser permitir al usuario, retirar al usuario, o rechazar el acceso del usuario.</p>	<p>Action :</p> <div style="border: 1px solid black; padding: 2px;"> Permit ▼ Permit Drop Reject </div>
<p>Paso 14:</p>	<p>Por último, seleccione la Hora en la que desea que se inicie el filtro y haga clic en Add/Apply</p>	<p>Time :</p> <p><input type="radio"/> Disable <input checked="" type="radio"/> Enable</p> <p>Begin time : 00 : 00</p> <p>End time : 00 : 00</p> <p>Begin day : Sun</p> <p>End day : Sun</p> <p style="text-align: right;"><input type="button" value="Add/Apply"/></p>

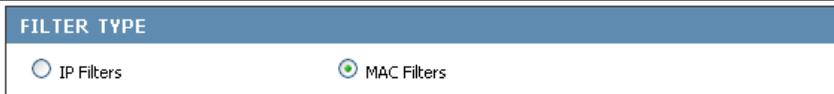


IMPORTANTE: Considere los escenarios que siguen al seleccionar la mejor opción. Una vez hecha una selección, tendrá que elegir entre variables automáticas. Tenga cuidado al realizar su selección, y sopesese también las ventajas y desventajas antes de tomar una decisión.

<p>Escenario 1</p>	<p>Si selecciona cualquier dirección IP obtendrá opciones similares en otros campos. Fíjese en las opciones de la imagen. Aquí, un usuario puede cambiar la dirección IP de origen, la dirección IP de destino y la Acción.</p>	<div style="border: 1px solid black; padding: 5px;"> <p>ADD FILTER</p> <p>Active IP Filter Rule : <input checked="" type="checkbox"/></p> <p>Name : <input type="text" value="example"/></p> <p>Interface : <input type="text" value="any"/></p> <p>Type : <input checked="" type="radio"/> Inbound <input type="radio"/> Outbound</p> <p>Protocol : <input type="text" value="any"/></p> <p>Source IP Address : <input type="text" value="any IP address"/></p> <p>Destination IP Address : <input type="text" value="any IP address"/></p> <p>Action : <input type="text" value="Permit"/></p> <p>Time :</p> <p><input type="radio"/> Disable <input checked="" type="radio"/> Enable</p> <p>Begin time : 00 : 00</p> <p>End time : 00 : 00</p> <p>Begin day : Sun</p> <p>End day : Sun</p> <p style="text-align: right;"><input type="button" value="Add/Apply"/></p> </div>
---------------------------	--	---

<p>Escenario 2</p>	<p>Si selecciona una dirección IP individual, automáticamente se creará un campo IP para que los usuarios introduzcan la IP individual correspondiente. Si selecciona un Puerto individual de origen, se creará también un campo para introducir el número del puerto individual.</p>		
<p>Escenario 3:</p>	<p>Si selecciona una dirección IP específica, automáticamente se crearán campos para la dirección IP de origen y la dirección IP de destino. Lo mismo ocurrirá si se selecciona un rango de puertos, con un número de puerto de origen y un número de puerto de destino.</p>		

La segunda opción en Tipo de filtro son los filtros MAC. En este caso las opciones son más sencillas, pero igual de efectivas. Vamos a ver las posibilidades.

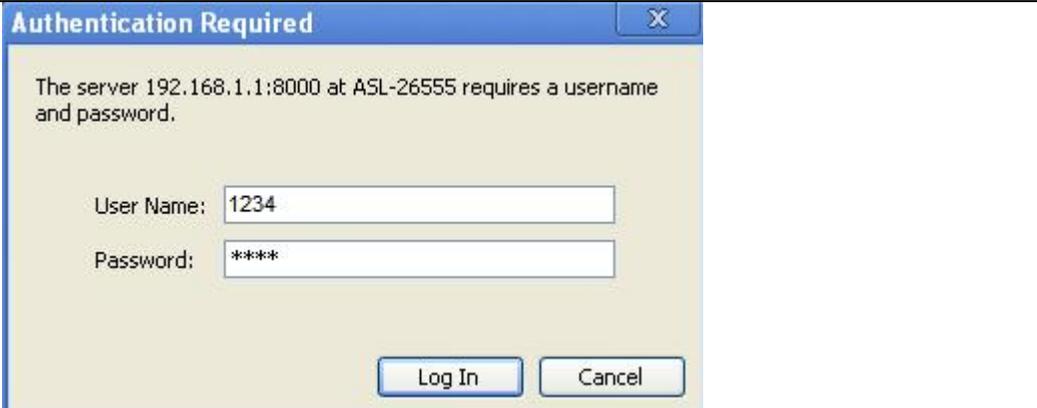
<p>Paso 1:</p>	<p>En Tipo de filtro, seleccione Filtros MAC</p>	
-----------------------	--	---

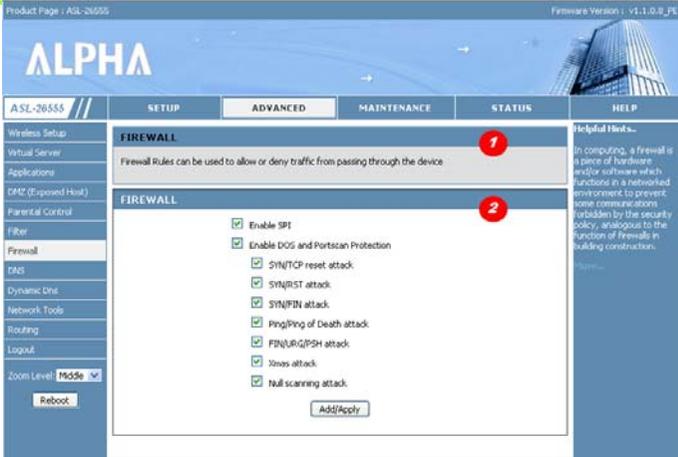
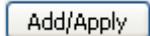
Paso 2:	<p>En Filtros MAC, existen tres opciones:</p> <ol style="list-style-type: none"> Deshabilitar Permitir Denegar <p>Si selecciona Filtros MAC deshabilitados, no se activará ningún filtrado.</p>	<input checked="" type="radio"/> Disabled MAC Filters <input type="radio"/> Only allow computers with MAC address listed below to access the network <input type="radio"/> Only deny computers with MAC address listed below to access the network												
Paso 3:	Haga clic en Permitir sólo ordenadores con dirección MAC...	<input checked="" type="radio"/> Only allow computers with MAC address listed below to access the network												
Paso 4:	Escriba un Nombre para identificar el Filtro	Name : <input type="text"/>												
Paso 5:	Escriba la dirección MAC del ordenador al que desea conceder permiso.  IMPORTANTE: Puede obtener la dirección MAC de un PC fijándose físicamente en la tarjeta PCI o con el comando IPCONFIG.	Name : <input type="text" value="TOPBITS"/> MAC Address : <input type="text" value="00"/> : <input type="text" value="0C"/> : <input type="text" value="F1"/> : <input type="text" value="56"/> : <input type="text" value="98"/> : <input type="text" value="AD"/>												
Paso 6:	Seleccione una Hora para habilitar el filtrado y haga clic en Add/Apply o Seleccione una hora de inicio y de fin.	Time : <input type="radio"/> Disable <input checked="" type="radio"/> Enable Begin time : <input type="text" value="01"/> : <input type="text" value="00"/> End time : <input type="text" value="12"/> : <input type="text" value="00"/> Begin day : <input type="text" value="Mon"/> End day : <input type="text" value="Fri"/> <input type="button" value="Add/Apply"/>												
Paso 7:	Cuando haya terminado de configurar al hora, haga clic en Add/Apply	<input type="button" value="Add/Apply"/>												
	Aparecerá una nueva tabla denominada Filtros MAC existentes . La tabla contendrá el Nombre , la dirección MAC y la Lista de eliminación . Para eliminar un Filtro MAC , marque la casilla de verificación Remove y haga clic en Remove selected .	<table border="1"> <thead> <tr> <th colspan="4">EXISTING MAC FILTERS</th> </tr> <tr> <th>Name</th> <th>MAC Address</th> <th>Remove</th> <th>Edit</th> </tr> </thead> <tbody> <tr> <td>TOPBITS</td> <td>00:0C:F1:56:98:AD</td> <td><input type="checkbox"/></td> <td><input type="radio"/></td> </tr> </tbody> </table> <input type="button" value="Remove Selected"/>	EXISTING MAC FILTERS				Name	MAC Address	Remove	Edit	TOPBITS	00:0C:F1:56:98:AD	<input type="checkbox"/>	<input type="radio"/>
EXISTING MAC FILTERS														
Name	MAC Address	Remove	Edit											
TOPBITS	00:0C:F1:56:98:AD	<input type="checkbox"/>	<input type="radio"/>											

Capítulo 19: Configuración del cortafuegos

Descripción general

Un **cortafuegos** es una parte de un sistema o red informática diseñado para bloquear los accesos no autorizados permitiendo al mismo tiempo las comunicaciones autorizadas. Se trata de un dispositivo o un conjunto de dispositivos configurados para permitir o denegar las transmisiones de red basándose en una serie de reglas y otros criterios. El cortafuegos del ASL-26555 permite una configuración mínima. La configuración resulta fácil e intuitiva. Siga estos pasos para habilitar el cortafuegos del ASL-26555.

Paso 1:	Abra el navegador y escriba la dirección IP por defecto del ASL-26555.	
Paso 2:	Escriba su Nombre de usuario y su Contraseña y haga clic en Log In .	
Paso 3:	Haga clic en Advanced, Firewall (Cortafuegos) .	

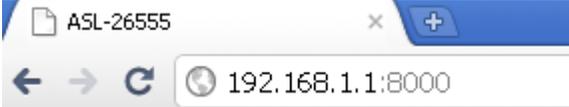
<p>Paso 4:</p>	<p>La interfaz Cortafuegos tiene dos ventanas:</p> <ol style="list-style-type: none"> 1. La primera ventana es la descripción 2. La segunda ventana es la herramienta de configuración 	
<p>Paso 5:</p>	<p>El ASL-26555 presenta nueve opciones para configurar el cortafuegos. Sigue una descripción de cada una de ellas:</p> <p>Habilitar SPI: SPI significa Inspección de paquetes de datos. Hace un seguimiento de las conexiones de la red y se fija en todos los paquetes entrantes tratando de concatenarlos con la solicitud original. Si el paquete no coincide, será rechazado. Habilite esta opción si desea comprobar todos los paquetes entrantes (consume muchos recursos de la CPU y puede ralentizar la red)</p> <p>Habilitar protección DOS y Portscan: significa Ataque de denegación de servicio. Su principal objetivo es tratar de hacer los recursos informáticos no disponibles para los usuarios. La protección Portscan impide que los atacantes encuentren puertos vulnerables abiertos.</p> <p>Ataque de reinicio SYN/TCP: este ataque trata de atacar el protocolo TCP y lo reinicia, acabando con la conexión. Algunas variantes similares son los ataques SYN/RST y SYN/FIN. Funcionan a niveles similares, pero su principal finalidad es atacar la pila TCP.</p>	

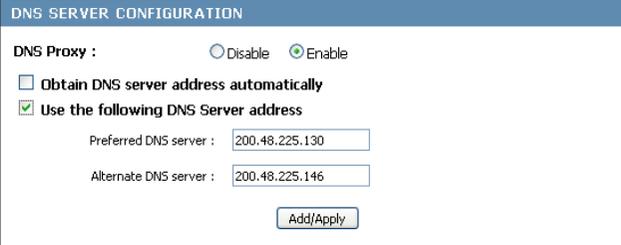
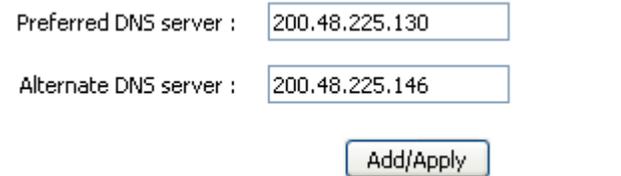
	<p>Ping/Ataque “ping de la muerte”: se trata de un ataque DOS en el que el atacante envía una solicitud de ping de más de 65.536 bytes. Este tamaño es superior al tamaño de un paquete normal. Crea una sobrecarga del buffer (algo similar a una inundación) en el sistema operativo que acaba con él.</p> <p>Ataques FIN/URG/PSH, Xmas y Null scanning: todos ellos atacan la pila TCP. Tratan de explotar pequeñas fisuras para diferenciar entre los puertos abiertos y cerrados.</p> <p>Puede encontrar más información acerca de estas amenazas en Internet, pero no hay que decir que la mayoría o todas ellas están clasificadas como amenazas para las redes.</p> <p>Seleccione las que desee aplicar o selecciónelas todas. Haga clic en Add/Apply para terminar.</p>	
--	---	--

Capítulo 20: Configuración de DNS y DNS dinámico

Descripción general

DNS significa Servicio de nombre de dominio. Su principal finalidad es traducir un nombre de dominio o URL en una dirección IP. Para configurar DNS, puede haber un servidor DNS presente localmente o en Internet. El ASL-26555 cuenta con una utilidad DNS muy sencilla. Veamos ahora cómo configurar los DNS.

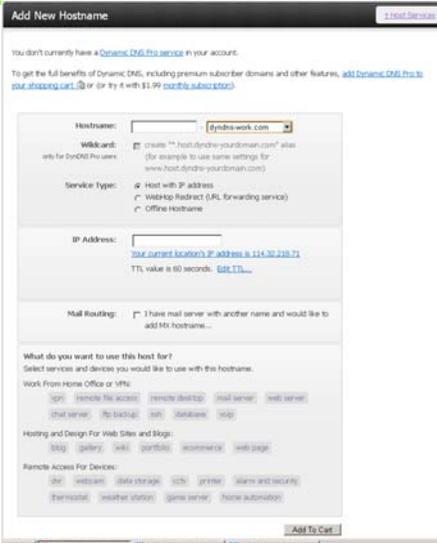
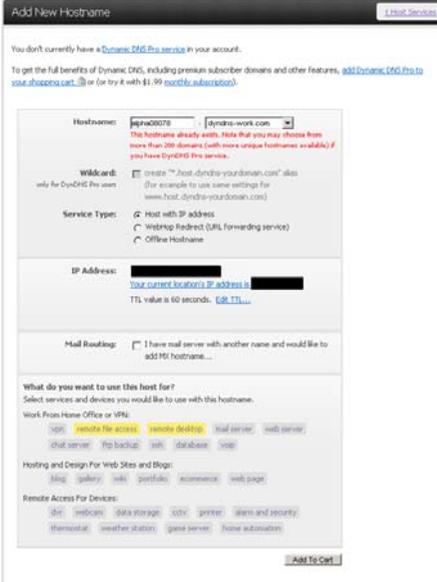
<p>Paso 1:</p>	<p>Abra el navegador y escriba la dirección IP por defecto del ASL-26555.</p>	
<p>Paso 2:</p>	<p>Escriba su Nombre de usuario y su Contraseña y haga clic en Log In.</p>	
<p>Paso 3:</p>	<p>Haga clic en Advanced,DNS.</p>	
<p>Paso 4:</p>	<p>La interfaz DNS tiene dos ventanas: 3. La primera ventana es la descripción 4. La segunda ventana es la herramienta de configuración</p>	

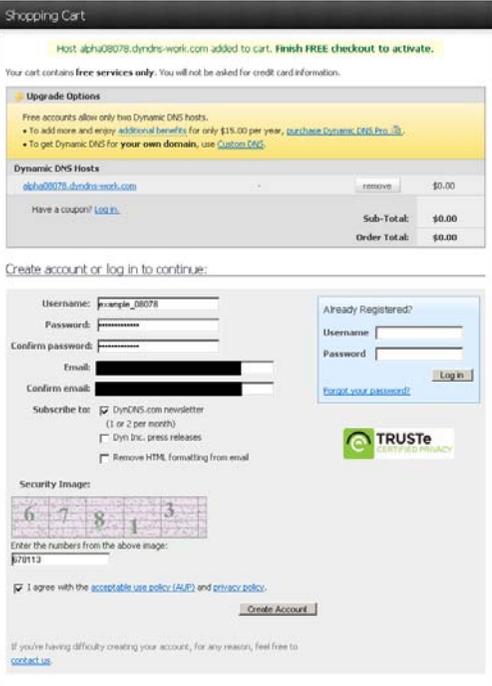
Paso 5:	Haga clic en Habilitar proxy DNS	
Paso 6:	Haga clic en Obtener la dirección del servidor DNS automáticamente y haga clic en Add/Apply .	
Para configurar manualmente el proxy DNS		
Paso 1:	Haga clic en Enable proxy DNS	
Paso 2:	Elimine la selección de Obtener la dirección del servidor DNS automáticamente y seleccione Utilizar la siguiente dirección de servidor DNS .	
Paso 3:	Escriba la dirección IP de su servidor DNS preferido y la dirección IP de un servidor DNS alternativo . Haga clic en Add/Apply cuando haya terminado.	

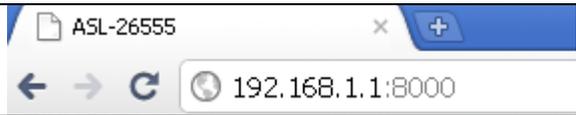
DNS dinámico

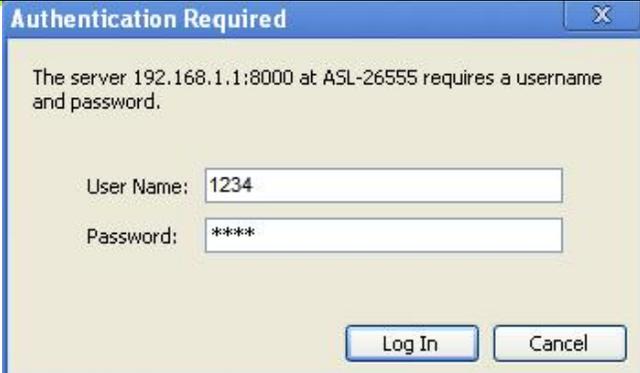
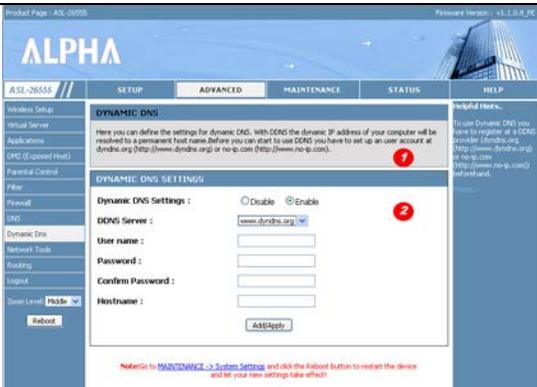
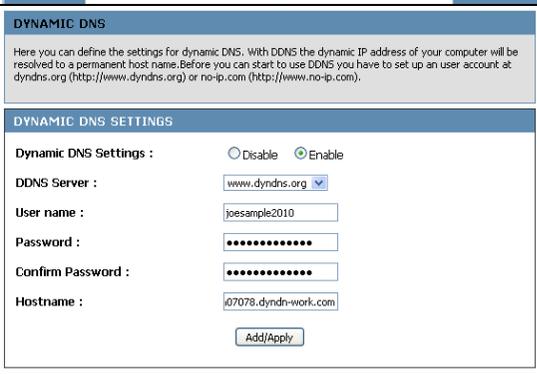
DNS dinámico es un servicio profesional que ofrece www.dyndns.com. Para utilizar este servicio, los usuarios deben registrarse en www.dyndns.com. El servicio permite básicamente crear un nombre de host para su ASL-26555. La ventaja de utilizar DNS dinámico es que resulta seguro y ofrece una mayor seguridad a su red. Ahora vamos a ver cómo configurar la ventana DNS dinámico. EL primer paso consiste en elegir entre dyndns o no-ip.

<p>Paso 1: Abra el navegador y escriba www.dyndns.com</p>		
<p>Paso 2: Abra una cuenta gratuita.</p>		

<p>Paso 3: Complete los requisitos de registro.</p>			
<p>Paso 4: Cumplimente el formulario.</p>			

<p>Paso 5:</p>	<p>Escriba su nombre de usuario y su contraseña.</p>	 <p>The screenshot shows a 'Shopping Cart' with one item: 'alpha08078.dynDNS-work.com' for \$0.00. Below the cart is a registration form with fields for Username, Password, Confirm password, Email, and Confirm email. There are checkboxes for newsletter subscription and a security image. A 'Create Account' button is visible at the bottom of the form.</p>
<p>Paso 6:</p>	<p>Compruebe su cuenta de correo electrónico.</p>	 <p>The screenshot shows the DynDNS website header with a search bar and navigation links. Below, it says 'One more step to go...' and 'We've sent an email to [redacted] to verify your account. Please check your inbox and click on the confirmation link.' There is a green arrow pointing to an email icon.</p>
<p>Paso 7:</p>	<p>Cuando responda al mensaje que le hayan enviado, su cuenta estará configurada.</p>	

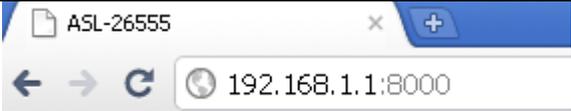
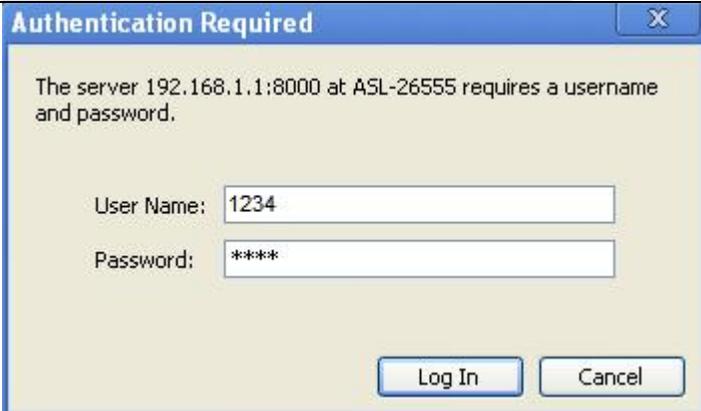
<p>Paso 8:</p>	<p>Abra el navegador y escriba la dirección IP por defecto del ASL-26555.</p>	 <p>The screenshot shows a browser window with the address bar containing '192.168.1.1:8000'. The browser tab is titled 'ASL-26555'.</p>
-----------------------	---	---

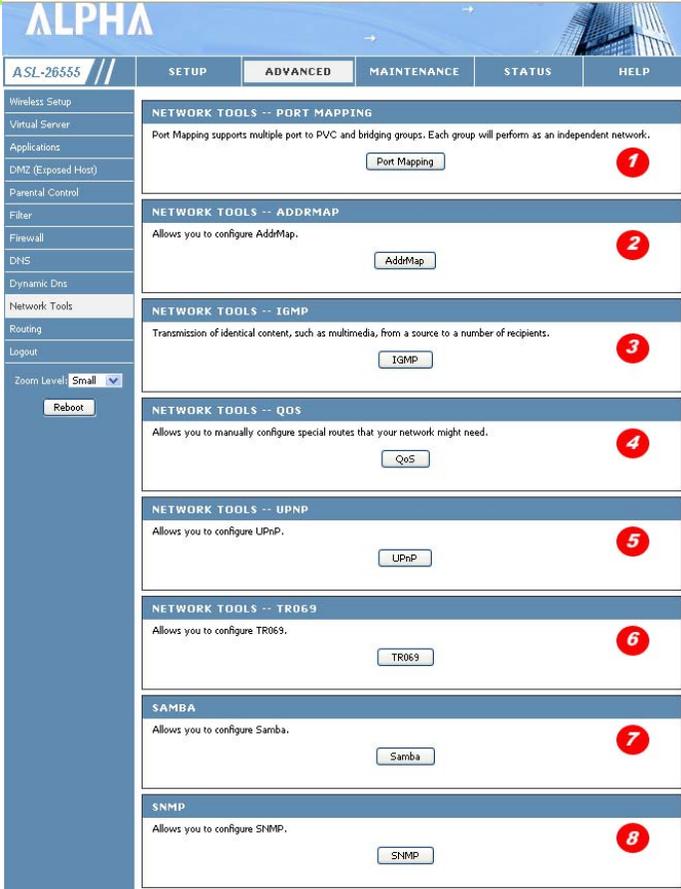
<p>Paso 9:</p>	<p>Escriba su Nombre de usuario y su Contraseña y haga clic en Log In.</p>	 <p>The server 192.168.1.1:8000 at ASL-26555 requires a username and password.</p> <p>User Name: 1234</p> <p>Password: ****</p> <p>Log In Cancel</p>
<p>Paso 10:</p>	<p>Haga clic en Advanced, Dynamic DNS (DNS dinámico).</p>	 <p>ADVANCED , Dynamic Dns</p>
<p>Paso 11:</p>	<p>La interfaz DNS dinámico tiene dos ventanas:</p> <ol style="list-style-type: none"> 1. La primera ventana es la descripción 2. La segunda ventana es la herramienta de configuración 	 <p>ALPHA</p> <p>ASL-26555 // SETUP ADVANCED MAINTENANCE STATUS HELP</p> <p>DYNAMIC DNS</p> <p>Here you can define the settings for dynamic DNS. With DDNS the dynamic IP address of your computer will be resolved to a permanent host name. Before you can start to use DDNS you have to set up an user account at dyndns.org (http://www.dyndns.org) or no-ip.com (http://www.no-ip.com).</p> <p>DYNAMIC DNS SETTINGS</p> <p>Dynamic DNS Settings : <input type="radio"/> Disable <input checked="" type="radio"/> Enable</p> <p>DDNS Server : www.dyndns.org</p> <p>User name : </p> <p>Password : </p> <p>Confirm Password : </p> <p>Hostname : </p> <p>Add/Apply</p>
<p>Paso 12:</p>	<p>Ahora, introduzca los datos que haya utilizado para la cuenta dyndns.</p>	 <p>DYNAMIC DNS</p> <p>Here you can define the settings for dynamic DNS. With DDNS the dynamic IP address of your computer will be resolved to a permanent host name. Before you can start to use DDNS you have to set up an user account at dyndns.org (http://www.dyndns.org) or no-ip.com (http://www.no-ip.com).</p> <p>DYNAMIC DNS SETTINGS</p> <p>Dynamic DNS Settings : <input type="radio"/> Disable <input checked="" type="radio"/> Enable</p> <p>DDNS Server : www.dyndns.org</p> <p>User name : joesample2010</p> <p>Password : </p> <p>Confirm Password : </p> <p>Hostname : 07078.dyndn-work.com</p> <p>Add/Apply</p>
<p>Paso 13:</p>	<p>Haga clic en Add/Apply para completar el proceso.</p>	 <p>Add/Apply</p>

Capítulo 21: Trabajar con herramientas de red

Descripción general

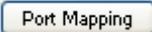
El ASL-26555 ofrece distintas herramientas de red. Cada herramienta mejora el ASL-26555 si se utiliza correctamente. A continuación conoceremos esas herramientas de red con esta guía paso a paso.

Paso 1:	Abra el navegador y escriba la dirección IP por defecto del ASL-26555.	
Paso 2:	Escriba su Nombre de usuario y su Contraseña y haga clic en Log In .	
Paso 3:	Haga clic en Advanced, Network Tools (Herramientas de red) .	

<p>Paso 4: En Herramientas de red, encontramos una lista con ocho herramientas</p> <ol style="list-style-type: none"> 1. Mapeo de puertos 2. AddrMap 3. IGMP 4. QOS 5. UPNP 6. TRO69 7. Samba 8. SNMP 	 <p>The screenshot shows the ALPHA router's web interface. The top navigation bar includes 'ASL-26555', 'SETUP', 'ADVANCED', 'MAINTENANCE', 'STATUS', and 'HELP'. The left sidebar lists various tools: Wireless Setup, Virtual Server, Applications, DMZ (Exposed Host), Parental Control, Filter, Firewall, DNS, Dynamic Dns, Network Tools, Routing, and Logout. The main content area is titled 'NETWORK TOOLS' and lists eight items, each with a description and a button: 1. Port Mapping (NETWORK TOOLS -- PORT MAPPING), 2. AddrMap (NETWORK TOOLS -- ADDRMAP), 3. IGMP (NETWORK TOOLS -- IGMP), 4. QoS (NETWORK TOOLS -- QOS), 5. UPnP (NETWORK TOOLS -- UPNP), 6. TR069 (NETWORK TOOLS -- TR069), 7. Samba (SAMBAs), and 8. SNMP (SNMP). A 'Reboot' button is visible at the bottom of the sidebar.</p>
---	--

Mapeo de puertos

El mapeo de puertos es una técnica para reenviar un paquete TCP/IP atravesando la puerta de enlace NAT hasta un puerto de red predeterminado en un host. Se emplea para permitir las comunicaciones de host externos con servicios suministrados en una LAN privada. El mapeo o reenvío de puertos permite a ordenadores remotos conectarse con un ordenador o servicio concreto dentro de una LAN privada, es decir, un usuario en casa que se comunica con un servidor en Internet.

<p>Paso 1: Haga clic en el botón Mapeo de puertos</p>	
---	---

Paso 2:	En CONFIGURACIÓN DE PORTMAP , vaya a Compatibilidad PortMap y haga clic en Enable	PORTMAP support : <input type="radio"/> Disable <input checked="" type="radio"/> Enable
Paso 3:	En la lista desplegable, seleccione uno de los canales PVC conectados a una de las LAN o dispositivos inalámbricos y haga clic en Add/Apply .	<div style="border: 1px solid gray; padding: 2px;"> None ▼ None PVC1 </div> , <input type="button" value="Add/Apply"/>

ADDRMAP

El mapeo de direcciones se emplea sobre todo en entornos corporativos en los que las NAT dinámicas son más habituales. En lugar de usar NAT estáticas (que ofrecen mapeo de direcciones IP internas a públicas uno a uno), las NAT dinámicas no hacen un mapeo estático de la dirección IP pública y suelen emplear un grupo de direcciones IP públicas disponibles. En este caso se emplea una tabla de direcciones IP conectadas a direcciones IP públicas. A continuación se explica esta configuración.

Paso 1:	Haga clic en el botón AddrMap en la sección o busque AddrMap en Herramientas de red	<input type="button" value="AddrMap"/>																		
Paso 2:	Haga clic en la casilla de verificación que hay junto a Habilitar regla de mapeo	Enable Mapping Rule : <input checked="" type="checkbox"/>																		
Paso 3:	Introduzca una dirección IP inicial y una dirección IP final	Internal Start Address : <input type="text"/> Internal End Address : <input type="text"/>																		
Paso 4:	Seleccione la Interfaz externa	<div style="border: 1px solid gray; padding: 2px;"> PVC1 ▼ PVC1 PVC2 PVC3 PVC4 PVC5 PVC6 PVC7 PVC8 </div>																		
Paso 5:	Escriba una Dirección externa y haga clic en Add/Apply	External Address : <input type="text" value="0.0.0.0"/>																		
Paso 6:	Aparecerá una Tabla de mapeo de direcciones debajo de los Ajustes de mapeo de direcciones .	<div style="border: 1px solid gray; padding: 5px;"> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th colspan="6">ADDRESS MAPPING TABLE</th> </tr> <tr> <th>Status</th> <th>Internal Address</th> <th>External Interface</th> <th>External Address</th> <th>Remove</th> <th>Edit</th> </tr> </thead> <tbody> <tr> <td>Active</td> <td>192.168.1.5-192.168.1.20</td> <td>PVC1</td> <td>114.32.218.71</td> <td><input type="checkbox"/></td> <td><input type="radio"/></td> </tr> </tbody> </table> <div style="text-align: center; margin-top: 5px;"><input type="button" value="Remove Selected"/></div> </div>	ADDRESS MAPPING TABLE						Status	Internal Address	External Interface	External Address	Remove	Edit	Active	192.168.1.5-192.168.1.20	PVC1	114.32.218.71	<input type="checkbox"/>	<input type="radio"/>
ADDRESS MAPPING TABLE																				
Status	Internal Address	External Interface	External Address	Remove	Edit															
Active	192.168.1.5-192.168.1.20	PVC1	114.32.218.71	<input type="checkbox"/>	<input type="radio"/>															
Paso 7:	Marque la casilla de verificación Remove y haga clic en Remove Selected para eliminar los ajustes de mapeo.	<input type="button" value="Remove Selected"/>																		

IGMP

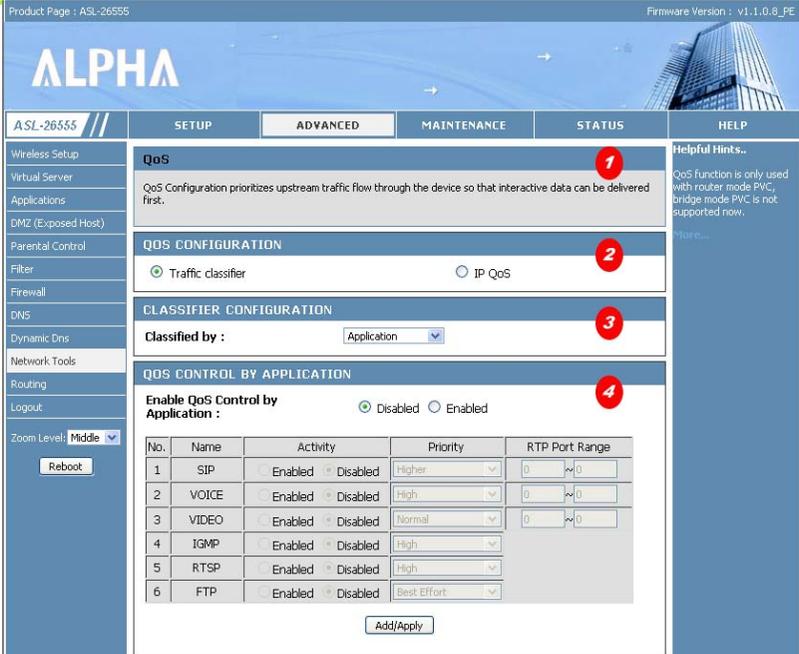
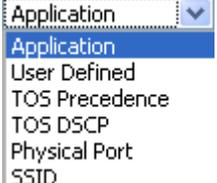
IGMP significa Protocolo de administración de grupos de Internet y es un protocolo de comunicación empleado por los hosts y los routers en las redes IP para crear grupos multidifusión. Se emplea sobre todo para el streaming de vídeo y los juegos online y permite un uso más eficiente de los recursos junto con este tipo de aplicaciones.

Paso 1:	Haga clic en el botón IGMP	
Paso 2:	Haga clic en el botón circular IGMP Proxy  IMPORTANTE: debe existir un proxy para utilizar esta función o transmitir datos desde un grupo	<input checked="" type="radio"/> IGMP Proxy
Paso 3:	Seleccione los botones IGMP no transparente o IGMP transparente .	<input checked="" type="radio"/> IGMP Non-transparent <input type="radio"/> IGMP Transparent
Paso 4:	Haga clic en Add/Apply para activar la herramienta	

Calidad de servicio (QOS)

Calidad de servicio (QOS) es la capacidad de conceder prioridades distintas a distintas aplicaciones, usuarios o flujos de datos o garantizar determinado nivel de rendimiento a un flujo de datos. Esto puede ser muy importante para servicios como el VOIP o las transmisiones de streaming en vivo. Estos servicios suelen precisar unas tasas de bits fijas y son sensibles al retardo. QOS resulta útil en zonas en las que la capacidad de red es un recurso limitado. Ahora veremos cómo se configura QOS en el ASL-26555.

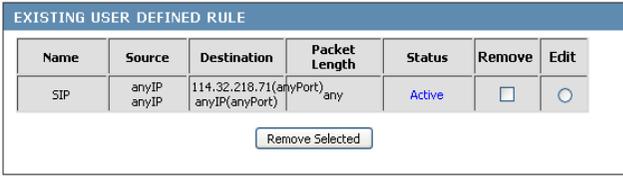
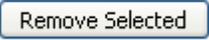
Paso 1:	Haga clic en el botón QOS	
----------------	----------------------------------	---

<p>Paso 2:</p>	<p>La interfaz QOS tiene cuatro ventanas:</p> <ol style="list-style-type: none"> 1. La primera ventana es la descripción 2. La segunda ventana es la herramienta de configuración de QOS 3. La tercera ventana es la Configuración del clasificador 4. La cuarta ventana es el Control por aplicación QOS 	
<p>Paso 3:</p>	<p>En Configuración QOS, haga clic en Clasificador de tráfico</p> <p> IMPORTANTE: Los clasificadores de tráfico de una red se refieren al tipo de flujo dentro de la misma. Normalmente, los clasificadores de tráfico operan sólo en una subred del tráfico.</p>	
<p>Paso 4:</p>	<p>En la lista desplegable de Configuración del clasificador, seleccione Aplicación</p>	
<p>Paso 5:</p>	<p>En Control por aplicación QOS, haga clic en Enabled</p>	

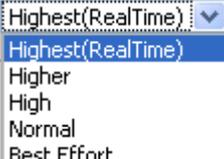
Paso 6:	Seleccione las Aplicaciones que desea habilitar, seleccione un nivel de prioridad en orden de importancia y escriba el rango de puertos RTP	<table border="1"> <thead> <tr> <th>No.</th> <th>Name</th> <th>Activity</th> <th>Priority</th> <th>RTP Port Range</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>SIP</td> <td><input checked="" type="radio"/> Enabled <input type="radio"/> Disabled</td> <td>Higher</td> <td>5060 ~ 5061</td> </tr> <tr> <td>2</td> <td>VOICE</td> <td><input checked="" type="radio"/> Enabled <input type="radio"/> Disabled</td> <td>Highest(RealTime)</td> <td>0 ~ 0</td> </tr> <tr> <td>3</td> <td>VIDEO</td> <td><input type="radio"/> Enabled <input checked="" type="radio"/> Disabled</td> <td>Normal</td> <td>0 ~ 0</td> </tr> <tr> <td>4</td> <td>IGMP</td> <td><input type="radio"/> Enabled <input checked="" type="radio"/> Disabled</td> <td>High</td> <td></td> </tr> <tr> <td>5</td> <td>RTSP</td> <td><input type="radio"/> Enabled <input checked="" type="radio"/> Disabled</td> <td>High</td> <td></td> </tr> <tr> <td>6</td> <td>FTP</td> <td><input type="radio"/> Enabled <input checked="" type="radio"/> Disabled</td> <td>Best Effort</td> <td></td> </tr> </tbody> </table>	No.	Name	Activity	Priority	RTP Port Range	1	SIP	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	Higher	5060 ~ 5061	2	VOICE	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	Highest(RealTime)	0 ~ 0	3	VIDEO	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	Normal	0 ~ 0	4	IGMP	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	High		5	RTSP	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	High		6	FTP	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	Best Effort	
No.	Name	Activity	Priority	RTP Port Range																																	
1	SIP	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	Higher	5060 ~ 5061																																	
2	VOICE	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	Highest(RealTime)	0 ~ 0																																	
3	VIDEO	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	Normal	0 ~ 0																																	
4	IGMP	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	High																																		
5	RTSP	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	High																																		
6	FTP	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	Best Effort																																		
Paso 7:	Haga clic en Add/Apply	<input type="button" value="Add/Apply"/>																																			

Existen distintas variantes para configurar QOS. Ahora veremos las demás opciones. **Definido por el usuario:**

Paso 1:	En la lista desplegable, seleccione Definido por el usuario .  IMPORTANTE: Como sugiere la opción, el usuario define las reglas de la aplicación.	<table border="1"> <thead> <tr> <th colspan="2">CLASSIFIER CONFIGURATION</th> </tr> </thead> <tbody> <tr> <td>Classified by :</td> <td>User Defined</td> </tr> </tbody> </table>	CLASSIFIER CONFIGURATION		Classified by :	User Defined																
CLASSIFIER CONFIGURATION																						
Classified by :	User Defined																					
Paso 2:	Seleccione Clasificador definido por el usuario habilitado	Enable User Defined Classifier : <input type="radio"/> Disabled <input checked="" type="radio"/> Enabled																				
Paso 3:	Marque la casilla de verificación Regla de aplicación activa	Active Application Rule : <input checked="" type="checkbox"/>																				
Paso 4:	Seleccione un nombre para la aplicación	Name : SIP																				
Paso 5:	Seleccione <ol style="list-style-type: none"> 1. un nivel de prioridad para la aplicación 2. Un protocolo – seleccione TODOS si no lo conoce 3. La dirección IP de origen (escriba una dirección IP conocida) 4. La dirección IP de destino (si la conoce) 5. La longitud del paquete (si la conoce) 	<table border="1"> <tbody> <tr> <td>Highest(RealTime)</td> <td>ALL</td> <td>any IP</td> <td>any</td> </tr> <tr> <td>Higher</td> <td>ALL</td> <td>any IP</td> <td>any</td> </tr> <tr> <td>High</td> <td>TCP</td> <td>Single IP Address</td> <td>any</td> </tr> <tr> <td>Normal</td> <td>UDP</td> <td>specify IP Address(Range)</td> <td>Single Length</td> </tr> <tr> <td>Best effort</td> <td>ICMP</td> <td>IP/Prefix Length</td> <td>Range</td> </tr> </tbody> </table>	Highest(RealTime)	ALL	any IP	any	Higher	ALL	any IP	any	High	TCP	Single IP Address	any	Normal	UDP	specify IP Address(Range)	Single Length	Best effort	ICMP	IP/Prefix Length	Range
Highest(RealTime)	ALL	any IP	any																			
Higher	ALL	any IP	any																			
High	TCP	Single IP Address	any																			
Normal	UDP	specify IP Address(Range)	Single Length																			
Best effort	ICMP	IP/Prefix Length	Range																			
Paso 6:	Haga clic en Add/Apply cuando haya terminado	<input type="button" value="Add/Apply"/>																				

<p>Paso 7: Aparecerá una tabla debajo de la ventana Regla definida por el usuario existente indicando que se ha creado una nueva regla. Esa regla puede eliminarse o editarse.</p>	
<p>Paso 8: Marque la casilla de verificación Remove y haga clic en Remove Selected para eliminar los ajustes de la regla.</p>	

Existen distintas variantes para configurar QOS. Ahora vamos a revisar las otras opciones. **Precedencia TOS:** significa **Tipo de servicio**. ¿Qué es? La intención de TOS es que el host remitente especifique una preferencia con respecto a la forma en que se debería administrar el datagrama cuando atraviese Internet. Un host podría configurar el valor del campo TOS como retardo bajo mientras que otro puede preferir una alta fiabilidad. Ahora vamos a aprender cómo se configurar la **Precedencia TOS**.

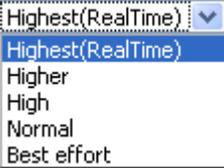
<p>Paso 1: En la lista desplegable, seleccione Precedencia TOS.</p>  <p>IMPORTANTE: Como sugiere la opción, el usuario define las reglas de la aplicación.</p>	
<p>Paso 2: Seleccione Habilitar clasificador de precedencia TOS</p>	<p>Enable ToS Precedence Classifier : <input type="radio"/> Disabled <input checked="" type="radio"/> Enabled</p>
<p>Paso 3: Marque la casilla de verificación Enable</p>	<p>Enable : <input checked="" type="checkbox"/></p>
<p>Paso 4: En los campos desde y hasta, introduzca el rango que desea configurar.</p>  <p>IMPORTANTE: En Precedencia TOS, puede configurar el rango de "0" a "7" o utilizar sólo un número. 0 e el valor por defecto, pero es preferible uno mayor.</p>	
<p>Paso 5: Seleccione una Prioridad en la lista desplegable</p>	
<p>Paso 6: Haga clic en Add/Apply</p>	

Existen distintas variantes para configurar QOS. Ahora vamos a revisar las otras opciones. **TOS DSCP**: significa **Tipo de servicio**. ¿Qué es? Se trata de una arquitectura de red que especifica un mecanismo sencillo, modular y de grano grueso para clasificar, administrar y ofrecer QOS en redes IP. Puede utilizarse desde para una latencia baja hasta para un tráfico de red crítico como la voz y el vídeo, ofreciendo al mismo tiempo unas garantías de tráfico sencillas a servicios no críticos como el tráfico web o la transferencia de archivos. Veamos ahora cómo configurar **TOS DSCP**

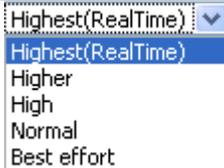
Paso 1: En la lista desplegable, seleccione TOS DSCP.  IMPORTANTE: Como sugiere la opción, el usuario define las reglas de la aplicación.		Classified by : <input type="text" value="TOS DSCP"/>																				
Paso 2: Seleccione Habilitar clasificador de TOS DSCP		Enable ToS DSCP Classifier : <input type="radio"/> Disabled <input checked="" type="radio"/> Enabled																				
Paso 3: Marque la casilla de verificación Enable		Enable : <input type="checkbox"/>																				
Paso 4: En los campos desde y hasta , introduzca el rango que desea configurar.  IMPORTANTE: En TOS DSCP , puede configurar el rango de "0" a "63" o utilizar sólo un número. 0 e el valor por defecto, pero es preferible uno mayor		<table border="1"> <thead> <tr> <th colspan="5">EXISTING DSCP LIST</th> </tr> <tr> <th>Status</th> <th>Priority</th> <th>Range</th> <th>Remove</th> <th>Edit</th> </tr> </thead> <tbody> <tr> <td>Active</td> <td>Highest(RealTime)</td> <td>1-9</td> <td><input type="checkbox"/></td> <td><input type="radio"/></td> </tr> <tr> <td>Inactive</td> <td>Higher</td> <td>20-30</td> <td><input type="checkbox"/></td> <td><input type="radio"/></td> </tr> </tbody> </table>	EXISTING DSCP LIST					Status	Priority	Range	Remove	Edit	Active	Highest(RealTime)	1-9	<input type="checkbox"/>	<input type="radio"/>	Inactive	Higher	20-30	<input type="checkbox"/>	<input type="radio"/>
EXISTING DSCP LIST																						
Status	Priority	Range	Remove	Edit																		
Active	Highest(RealTime)	1-9	<input type="checkbox"/>	<input type="radio"/>																		
Inactive	Higher	20-30	<input type="checkbox"/>	<input type="radio"/>																		
Paso 5: Seleccione una Prioridad en la lista desplegable		<input type="text" value="Highest(RealTime)"/> <ul style="list-style-type: none"> Highest(RealTime) Higher High Normal Best Effort 																				
Paso 6: Haga clic en Add/Apply		<input type="button" value="Add/Apply"/>																				

Existen distintas variantes para configurar QOS. Ahora vamos a revisar las otras opciones. **Puerto físico**: ¿Qué es? El puerto físico gestiona QOS en un puerto físico específico. Ahora vamos a ver cómo se configura el **Puerto físico**

Paso 1: En la lista desplegable, seleccione Puerto físico .  IMPORTANTE: Como sugiere la opción, el usuario define las reglas de la aplicación.		Classified by : <input type="text" value="Physical Port"/>
--	--	---

Paso 2:	Seleccione Habilitar control QOS mediante puerto físico	Enable QoS Control by Physical Port : <input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
Paso 3:	Seleccione la Prioridad desde cada puerto LAN	LAN1 : <input type="text" value="Highest(RealTime)"/> , 
Paso 4:	Haga clic en Add/Apply	<input type="button" value="Add/Apply"/>

Existen distintas variantes para configurar QOS. Ahora vamos a revisar las otras opciones. **SSID:** ¿Qué es? SSID gestiona QOS en una red inalámbrica. Ahora vamos a ver cómo se configura la **SSID**

Paso 1:	En la lista desplegable, seleccione SSID.  IMPORTANTE: Como sugiere la opción, el usuario define las reglas de la aplicación.	Classified by : <input type="text" value="SSID"/>
Paso 2:	Seleccione Habilitar control QOS mediante SSID	Enable QoS Control by SSID : <input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
Paso 3:	Seleccione la Prioridad desde la SSID.	SSID1 : <input type="text" value="Highest(RealTime)"/> , 
Paso 4:	Haga clic en Add/Apply	<input type="button" value="Add/Apply"/>

Existen distintas variantes para configurar QOS. Ahora vamos a revisar las otras opciones. La última técnica de configuración es IP QOS. IP QOS dedica QOS a direcciones IP específicas. Controla el ancho de banda y los niveles de prioridad para el tráfico de subida y convierte en prioritarios los datos interactivos.

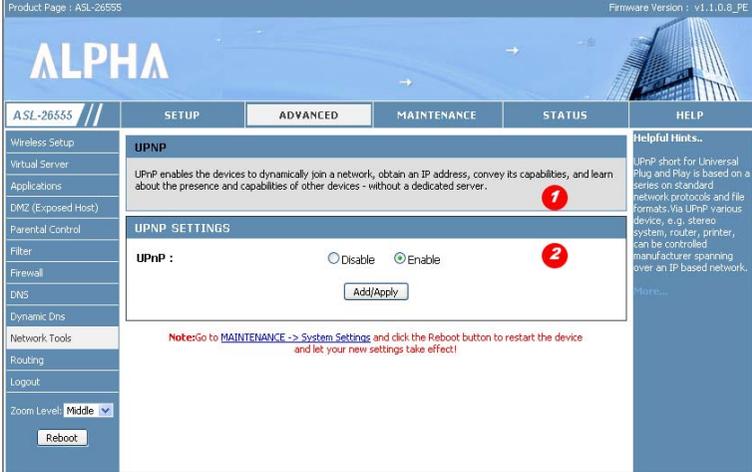
Paso 1:	En Configuración QOS haga clic en QOS IP	
Paso 2:	En Configuración QOS IP , seleccione la Interfaz en la lista desplegable	Interface : <input type="text" value="PVC1"/>

Paso 3:	Haga clic en Enable para habilitar la interfaz	Enable : <input type="radio"/> Disabled <input checked="" type="radio"/> Enabled																		
Paso 4:	Seleccione el Ancho de banda . Seleccione Auto o escriba una velocidad específica	Bandwidth : <input checked="" type="radio"/> Auto <input type="radio"/> <input type="text"/> Kbps																		
Paso 5:	La tabla puede configurarse por separado pero sirve solamente con orientación.	<table border="1"> <thead> <tr> <th>Enable</th> <th>Priority</th> <th>Weight</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/></td> <td>Highest(RealTime)</td> <td></td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td>Higher</td> <td><input type="text" value="40"/> %</td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td>High</td> <td><input type="text" value="30"/> %</td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td>Normal</td> <td><input type="text" value="20"/> %</td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td>Best Effort</td> <td><input type="text" value="10"/> %</td> </tr> </tbody> </table>	Enable	Priority	Weight	<input checked="" type="checkbox"/>	Highest(RealTime)		<input checked="" type="checkbox"/>	Higher	<input type="text" value="40"/> %	<input checked="" type="checkbox"/>	High	<input type="text" value="30"/> %	<input checked="" type="checkbox"/>	Normal	<input type="text" value="20"/> %	<input checked="" type="checkbox"/>	Best Effort	<input type="text" value="10"/> %
Enable	Priority	Weight																		
<input checked="" type="checkbox"/>	Highest(RealTime)																			
<input checked="" type="checkbox"/>	Higher	<input type="text" value="40"/> %																		
<input checked="" type="checkbox"/>	High	<input type="text" value="30"/> %																		
<input checked="" type="checkbox"/>	Normal	<input type="text" value="20"/> %																		
<input checked="" type="checkbox"/>	Best Effort	<input type="text" value="10"/> %																		
Paso 6:	Haga clic en Add/Apply cuando haya terminado	<input type="button" value="Add/Apply"/>																		

Universal Plug n Play (UPnP)

Universal Plug and Play es un conjunto de protocolos de red que permite a los dispositivos conectados en red como impresoras, PC y dispositivos Wi-Fi descubrir directamente la presencia de los otros en la red y establecer servicios de red funcionales para compartir datos, comunicaciones y entretenimiento. Ahora vamos a ver cómo se configura **UPnP**.

Paso 1:	Haga clic en el botón UPnP	<input type="button" value="UPnP"/>
----------------	-----------------------------------	-------------------------------------

<p>Paso 2:</p>	<p>La interfaz UPnP tiene dos ventanas:</p> <ol style="list-style-type: none"> 1. La primera ventana es la descripción 2. La segunda ventana es la herramienta de configuración de UPnP 	
<p>Paso 3:</p>	<p>En Configuración UPnP, haga clic en Enable</p>	<p>UPnP : <input type="radio"/> Disable <input checked="" type="radio"/> Enable</p>
<p>Paso 4:</p>	<p>Haga clic en Add/Apply</p>	<p><input type="button" value="Add/Apply"/></p>

TR069

TR-069 es un foro que define un protocolo de capa de aplicación para la administración remota de dispositivos de usuario final. Como protocolo bidireccional, permite la comunicación entre los equipos de las instalaciones del cliente y los servidores de configuración automática. Todos nuestros equipos modernos como routers, decodificadores y teléfonos VOIP utilizan TR-069 para autenticarse entre sí y con las estaciones de base. Esto se hace automáticamente con este estándar.

<p>Paso 1:</p>	<p>Haga clic en el botón TR069</p>	<p><input type="button" value="TR069"/></p>
-----------------------	---	---

<p>Paso 2:</p>	<p>La interfaz TR069 tiene dos ventanas:</p> <ol style="list-style-type: none"> 1. La primera ventana es la descripción 2. La segunda ventana es la herramienta de configuración de TR069 	
<p>Paso 3:</p>	<p>En TR069, marque la casilla de verificación</p>	<p>TR069 : <input checked="" type="checkbox"/></p>
<p>Paso 4:</p>	<p>Introduzca un Nombre de usuario</p>	<p>Username : <input type="text"/></p>
<p>Paso 5:</p>	<p>Escriba una Contraseña</p>	<p>Password : <input type="password"/></p>
<p>Paso 6:</p>	<p>Escriba una URL ACS o la URL ACS por defecto</p> <p> IMPORTANTE: Una URL ACS procede del servidor ACS. Para configurar TR069, debe autenticarse con un servidor ACS</p>	<p>ACS URL : <input type="text" value="http://200.48.229.23:7003/cwmpWeb/c"/></p> <p>Default ACS URL : <input type="text"/></p>
<p>Paso 7:</p>	<p>Escriba una URL CPE</p> <p> IMPORTANTE: CPE significa Equipo de las instalaciones del cliente y se trata de un terminal o cualquier otro equipo situado en las instalaciones del abonado y conectado con un canal de telecomunicación en el punto de demarcación. La demarcación es un punto establecido en un edificio</p>	<p>CPE URL : <input type="text" value="http://5.51.33.20:7547/alpha"/></p>

	para separar los equipos del cliente de los equipos de la compañía telefónica. Un ejemplo de CPE es el iPhone	
Paso 8:	En Configuración de información , seleccione Periódica	Inform Configure : <input type="radio"/> Disable <input checked="" type="radio"/> Periodic
Paso 9:	Introduzca el número de Intervalos periódicos por segundo	Periodic Interval : <input type="text" value="300"/> <i>Seconds</i>
Paso 10:	Para configurar un Tiempo de información periódico , seleccione Enable	Periodic Inform Time <input type="radio"/> Disable <input checked="" type="radio"/> Enable
Paso 11:	Los usuarios pueden introducir un calendario con meses, días y años o configurar el servidor hasta el último segundo.	Month : <input type="text" value="Jan"/> Day : <input type="text" value="1"/> Year : <input type="text" value="2002"/> Hour : <input type="text" value="8"/> Minute : <input type="text" value="0"/> Second : <input type="text" value="0"/>
Paso 12:	Para utilizar un servidor STUN introduzca los detalles en los espacios correspondientes. Su proveedor de servicios podrá darle esos datos.	STUN ENABLE : <input type="radio"/> Disable <input checked="" type="radio"/> Enable STUN SERVER ADDRESS : <input type="text" value="stun.voipbuster.com"/> STUN SERVER PORT : <input type="text" value="3478"/> STUN USERNAME : <input type="text" value="john"/> STUN PASSWORD : <input type="password" value="*****"/> STUN UDP LISTEN PORT : <input type="text" value="3478"/>
Paso 13:	Haga clic en Add/Apply	<input type="button" value="Add/Apply"/>

Samba

Samba es un protocolo utilizado para comunicarse con PC y equipos UNIX. Normalmente se emplea para compartir archivos y servicios de impresión e incorpora numerosos servicios y protocolos. Samba configura cuotas de red para directorios UNIX seleccionados. Estos directorios se muestran a los usuarios de Microsoft Windows como carpetas de Windows normales a las que puede accederse a través de la red. Ahora vamos a ver cómo se configura **Samba**.

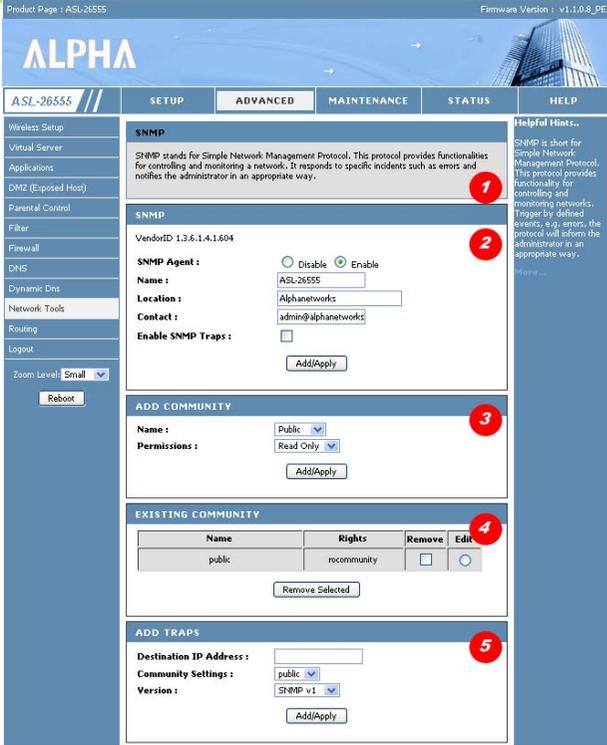
Paso 1:	Haga clic en el botón Samba	<input type="button" value="Samba"/>
----------------	------------------------------------	--------------------------------------

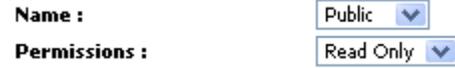
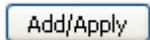
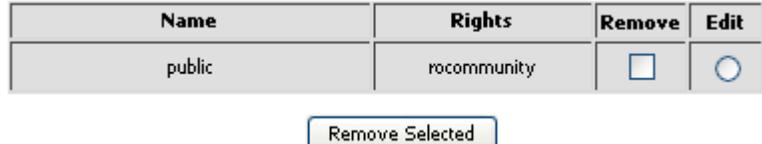
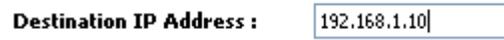
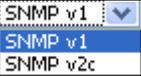
Paso 2:	La interfaz Samba tiene tres ventanas: 1. La primera ventana es la descripción 2. La segunda ventana es la herramienta de configuración de TR069 3. La tercera ventana es el Dispositivo montado	
Paso 3:	En Samba , haga clic en Enable	Enable : <input type="radio"/> Disable <input checked="" type="radio"/> Enable
Paso 4:	Escriba un Nombre NetBIOS	NetBIOS Name : <input type="text" value="ASL-26555"/>
Paso 5:	Introduzca el Grupo de trabajo al que se está conectando	Workgroup : <input type="text" value="Home"/>
Paso 6:	Haga clic en Add/Apply	<input type="button" value="Add/Apply"/>
Paso 7:	En Desmontar USB , haga clic en el botón desmontar para liberar el dispositivo	<input type="button" value="Unmount"/>

SNMP

SNMP significa Protocolo simple de administración de red. Suele emplearse sobre todo en sistemas de administración de redes para controlar los dispositivos conectados a la red que precisan ser administrados. Básicamente, SNMP expone los datos de administración en la red. Ahora veremos cómo se configura SNMP.

Paso 1:	Haga clic en el botón SNMP	<input type="button" value="SNMP"/>
----------------	-----------------------------------	-------------------------------------

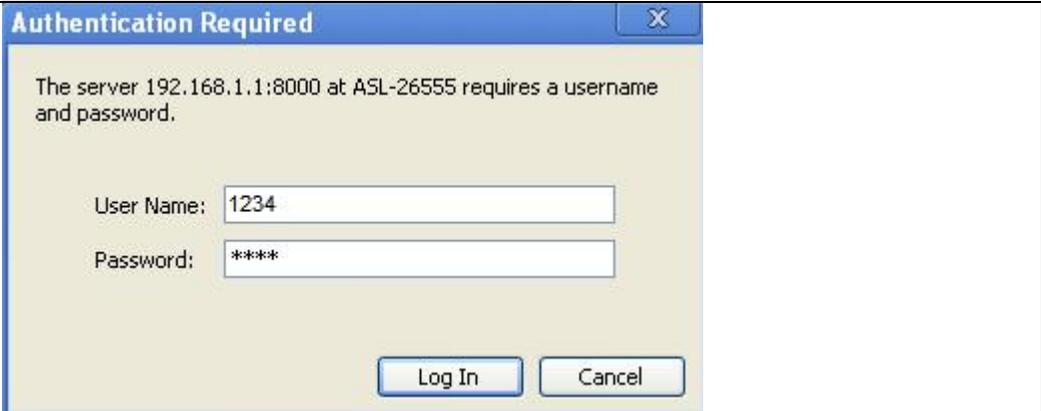
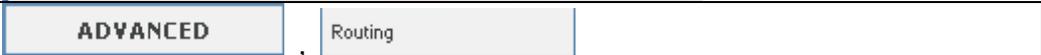
	<p>Paso 2: La interfaz SNMP tiene cinco ventanas:</p> <ol style="list-style-type: none"> 1. La primera ventana es la descripción 2. La segunda ventana es la herramienta de configuración de SNMP 3. La tercera ventana es el campo Añadir comunidad 4. La cuarta ventana es el campo Comunidad existente 5. La quinta ventana es el campo Añadir trampas 	
<p>Paso 3:</p>	<p>Para seleccionar un Agente SNMP, haga clic en Enable</p>	<p>SNMP Agent : <input type="radio"/> Disable <input checked="" type="radio"/> Enable</p>
<p>Paso 4:</p>	<p>Introduzca el nombre del servidor SNMP</p>	<p>Name : <input type="text" value="ASL-26555"/></p>
<p>Paso 5:</p>	<p>Dé un nombre a la ubicación del servidor SNMP en la red</p>	<p>Location : <input type="text" value="Alpha"/></p>
<p>Paso 6:</p>	<p>Escriba una dirección de e-mail en el campo Contacto</p>	<p>Contact : <input type="text" value="[REDACTED]"/></p>
<p>Paso 7:</p>	<p>Marque la casilla de verificación debajo de Habilitar trampas SNMP</p>	<p>Enable SNMP Traps : <input checked="" type="checkbox"/></p>
<p>Paso 8:</p>	<p>Haga clic en Add/Apply</p>	<p><input type="button" value="Add/Apply"/></p>
	<p>Para añadir el servidor SNMP a una comunidad</p>	

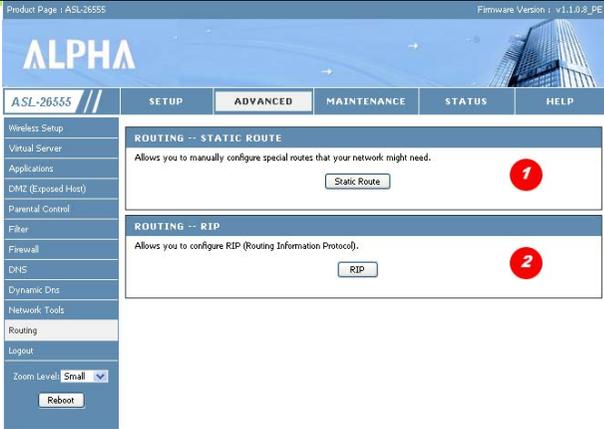
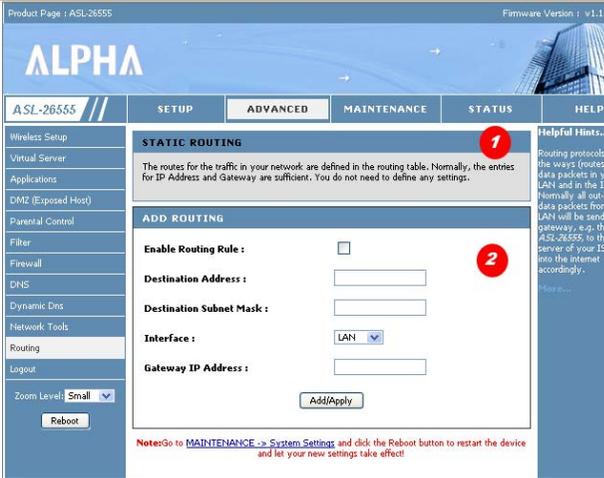
<p>Paso 1:</p>	<p>En Nombre, seleccione Privado o Público en la lista desplegable</p>	
<p>Paso 2:</p>	<p>En Permiso, seleccione Sólo lectura</p>	
<p>Paso 3:</p>	<p>Haga clic en Add/Apply para añadirlo a la tabla</p>	
<p>Paso 4:</p>	<p>Para eliminar un dispositivo de la Comunidad SNMP, marque la casilla de verificación Remove y haga clic en Remove Selected</p>	
<p>Paso 5:</p>	<p>Para Añadir trampas, escriba una dirección IP en la misma subred</p>	
<p>Paso 6:</p>	<p>Seleccione Público o Privado en Configuración de la comunidad</p>	
<p>Paso 7:</p>	<p>Seleccione la versión de SNMP</p>	
<p>Paso 8:</p>	<p>Haga clic en Add/Apply</p>	
<p>Paso 9:</p>	<p>Para eliminar una trampa existente, marque la casilla de verificación Remove y haga clic en Remove Selected.</p>	

Capítulo 22: Configuración del enrutamiento

Descripción general

El enrutamiento es el proceso de selección de rutas en una red a través de las cuales enviar el tráfico de la misma. En las redes de paquetes conmutados, el enrutamiento dirige el reenvío de los paquetes desde su origen hacia su destino último a través de dispositivos de hardware como el ASL-26555. Veamos ahora cómo configurar el enrutamiento.

Paso 1:	Abra el navegador y escriba la dirección IP por defecto del ASL-26555.	
Paso 2:	Escriba su Nombre de usuario y su Contraseña y haga clic en Log In .	
Paso 3:	Haga clic en Advanced, Routing (Enrutamiento) .	

<p>Paso 4: La interfaz Routing tiene dos ventanas:</p> <ol style="list-style-type: none"> 1. La primera ventana corresponde al Enrutamiento estático 2. La segunda ventana corresponde al Protocolo de información de enrutamiento 		
<p>Paso 5: Haga clic en el botón Static Route (Enrutamiento estático)</p>		
<p>Paso 6: La interfaz Static Route (Enrutamiento estático) tiene tres ventanas:</p> <ol style="list-style-type: none"> 1. La primera ventana es la descripción 2. La segunda ventana es el cuadro de configuración Añadir enrutamiento 		
<p>Paso 7: En Añadir enrutamiento, marque la casilla de verificación Habilitar regla de enrutamiento</p>		<p>Enable Routing Rule : <input checked="" type="checkbox"/></p>
<p>Paso 8: Escriba una Dirección IP de destino</p>		<p>Destination Address : <input type="text" value="192.168.1.50"/></p>
<p>Paso 9: Introduzca una Máscara de subred</p>		<p>Destination Subnet Mask : <input type="text" value="255.255.255.0"/></p>
<p>Paso 10: Seleccione la Interfaz</p>		<p>Interface : <input type="text" value="LAN"/></p>

Paso 11:	Escriba la Dirección IP de la puerta de enlace por defecto	Gateway IP Address : <input type="text" value="192.168.1.254"/>														
Paso 12:	Haga clic en Add/Apply	<input type="button" value="Add/Apply"/>														
Paso 13:	La Tabla de enrutamiento aparece después de hacer clic en el botón Add/Apply	<div data-bbox="1099 284 1794 533"> <p>ROUTING TABLE</p> <table border="1"> <thead> <tr> <th>Status</th> <th>Network</th> <th>Destination Subnet Mask</th> <th>Interface</th> <th>Gateway</th> <th>Remove</th> <th>Edit</th> </tr> </thead> <tbody> <tr> <td>Active</td> <td>192.168.1.50</td> <td>255.255.255.0</td> <td>LAN</td> <td>192.168.1.254</td> <td><input type="checkbox"/></td> <td><input type="radio"/></td> </tr> </tbody> </table> <p><input type="button" value="Remove Selected"/></p> </div>	Status	Network	Destination Subnet Mask	Interface	Gateway	Remove	Edit	Active	192.168.1.50	255.255.255.0	LAN	192.168.1.254	<input type="checkbox"/>	<input type="radio"/>
Status	Network	Destination Subnet Mask	Interface	Gateway	Remove	Edit										
Active	192.168.1.50	255.255.255.0	LAN	192.168.1.254	<input type="checkbox"/>	<input type="radio"/>										
Paso 14:	Para eliminar un elemento de la tabla de enrutamiento, marque la casilla de verificación bajo Remove y haga clic en Remove Selected	<div data-bbox="1099 545 1794 794"> <p>ROUTING TABLE</p> <table border="1"> <thead> <tr> <th>Status</th> <th>Network</th> <th>Destination Subnet Mask</th> <th>Interface</th> <th>Gateway</th> <th>Remove</th> <th>Edit</th> </tr> </thead> <tbody> <tr> <td>Active</td> <td>192.168.1.50</td> <td>255.255.255.0</td> <td>LAN</td> <td>192.168.1.254</td> <td><input checked="" type="checkbox"/></td> <td><input type="radio"/></td> </tr> </tbody> </table> <p><input type="button" value="Remove Selected"/></p> </div> <p data-bbox="1099 801 1783 842">Notes:Go to MAINTENANCE -> System Settings and click the Reboot button to restart the device and let your new settings take effect!</p>	Status	Network	Destination Subnet Mask	Interface	Gateway	Remove	Edit	Active	192.168.1.50	255.255.255.0	LAN	192.168.1.254	<input checked="" type="checkbox"/>	<input type="radio"/>
Status	Network	Destination Subnet Mask	Interface	Gateway	Remove	Edit										
Active	192.168.1.50	255.255.255.0	LAN	192.168.1.254	<input checked="" type="checkbox"/>	<input type="radio"/>										

Para configurar el **Protocolo de información de enrutamiento (RIP)**, siga estos pasos:

Paso 1:	Haga clic en el botón RIP	<input type="button" value="RIP"/>
----------------	----------------------------------	------------------------------------

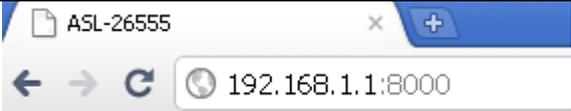
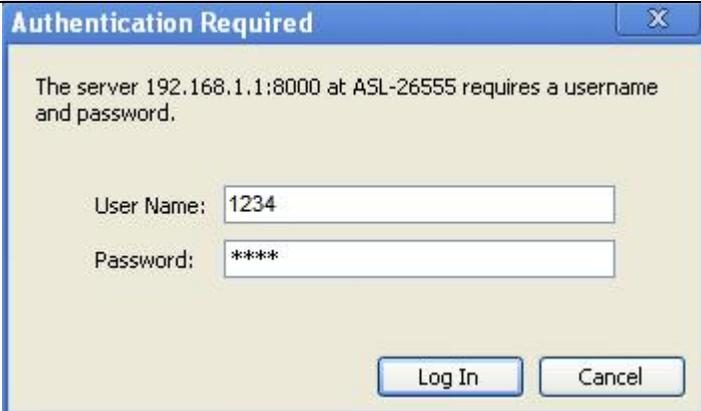
<p>Paso 2: La interfaz Protocolo de información de enrutamiento tiene dos ventanas:</p> <ol style="list-style-type: none"> 1. La primera ventana es la descripción 2. La segunda ventana es el cuadro de configuración RIP 	
<p>Paso 3: Haga clic en Enable en Habilitar RIP</p>	<p>Enable Rip : <input type="radio"/> Disable <input checked="" type="radio"/> Enable</p>
<p>Paso 4: Seleccione una Interfaz en la lista desplegable</p>	<p>PVC1 ▾ PVC1 PVC2 PVC3 PVC4 PVC5 PVC6 PVC7 PVC8 LAN</p>
<p>Paso 5: Haga clic en Enable en la sección Habilitar entrante</p>	<p>Enable In-bound : <input checked="" type="radio"/> Disable <input type="radio"/> Enable</p>
<p>Paso 6: Seleccione un Protocolo en el menú desplegable</p>	<p>RIP v1 only ▾ RIP v1 only RIP v2 only RIP v1 & v2 Both</p>
<p>Paso 7: Haga clic en Enable en la sección Habilitar saliente</p>	<p>Enable Out-bound : <input type="radio"/> Disable <input checked="" type="radio"/> Enable</p>
<p>Paso 8: Selección un Protocolo en el menú desplegable</p>	<p>RIP v1 only ▾ RIP v1 only RIP v2 only RIP v1 & v2 Both</p>
<p>Paso 9: Haga clic en Add/Apply</p>	<p>Add/Apply</p>

Con esto terminan los ajustes de configuración de la interfaz **Avanzado**. Muchas de las funciones de esta página tienen enlaces con otras páginas. Durante la configuración, asegúrese de comprender los procesos claramente y de saber cómo esos cambios afectan a las otras ventanas de interfaz.

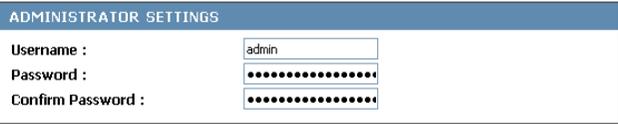
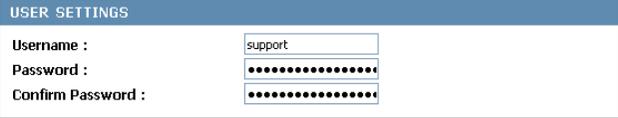
Capítulo 23: Mantenimiento

Descripción general

La sección Mantenimiento es el sistema nervioso central del ASL-26555. Todas las funciones de administración se configuran aquí. El sistema está limitado a un número de configuraciones que puede realizarse en la sección mantenimiento, pero, como su propio nombre indica, se trata de la sección de mantenimiento. Ahora vamos a ver qué hay en la ventana Mantenimiento.

<p>Paso 1:</p>	<p>Abra el navegador y escriba la dirección IP por defecto del ASL-26555.</p>	
<p>Paso 2:</p>	<p>Escriba su Nombre de usuario y su Contraseña y haga clic en Log In.</p>	
<p>Paso 3:</p>	<p>Haga clic en Maintenance (Mantenimiento), la primera interfaz que aparecerá es la ventana de administración.</p>	

<p>Paso 4: En Administration (Administración), hay cuatro ventanas:</p> <ol style="list-style-type: none"> 1. La primera ventana es la descripción 2. La segunda ventana corresponde a los Ajustes del administrador 3. La segunda ventana corresponde a los Ajustes del usuario 4. La cuarta ventana es la Administración remota 	
---	---

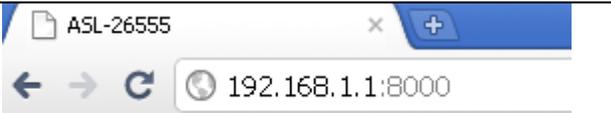
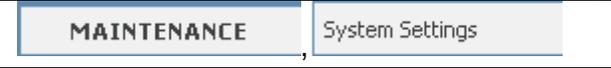
<p>Ajustes del administrador:</p> <p>Contiene el nombre de usuario del administrador, su contraseña y la confirmación de la contraseña.</p> <p> IMPORTANTE: Esta información aparecerá automáticamente cuando entre en la sección de mantenimiento</p>	
<p>Ajustes del usuario:</p> <p>Contiene el nombre de usuario, la contraseña y la confirmación de la contraseña.</p> <p> IMPORTANTE: Esta información aparecerá automáticamente cuando entre en la sección de</p>	

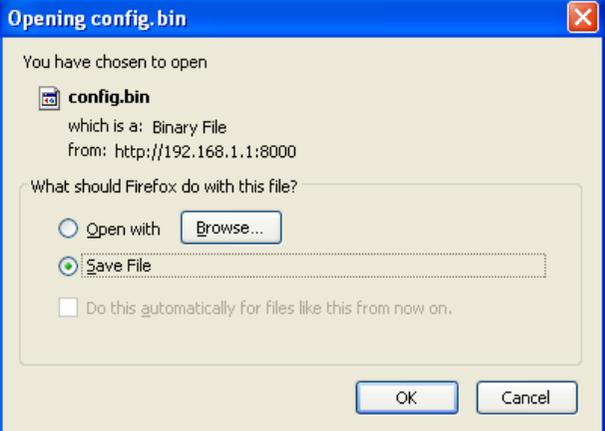
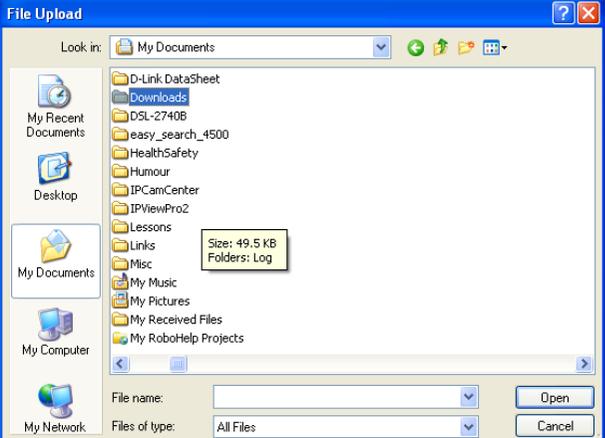
	mantenimiento	
	Administración remota: Haga clic en Enable , en el HTTP: (MHS GUI)  IMPORTANTE: Esto abrirá la interfaz Amper Easy User. Consulte a un administrador de sistemas si desea utilizar esa interfaz	HTTP :(MHS GUI) <input type="radio"/> Disable <input checked="" type="radio"/> Enable
Paso 2:	Escriba la dirección IP y el número de puerto	IP/Prefix length : <input type="text" value="0.0.0.0"/> / <input type="text" value="0"/> Port : <input type="text" value="80"/>
Paso 3:	Habilite la GUI ALPHA , y haga clic en Enable en la HTTP: (GUI ALPHA)	HTTP :(ALPHA GUI) <input type="radio"/> Disable <input checked="" type="radio"/> Enable
Paso 4:	Escriba la dirección IP y el número de puerto si fuera preciso.	IP/Prefix length : <input type="text" value="0.0.0.0"/> / <input type="text" value="0"/> Port : <input type="text" value="8000"/>
Paso 5:	Habilite la función TELNET , haga clic en Enable	TELNET : <input type="radio"/> Disable <input checked="" type="radio"/> Enable
Paso 6:	Escriba la dirección IP del TELNET de destino	IP/Prefix length : <input type="text" value="0.0.0.0"/> / <input type="text" value="0"/>
Paso 7:	En FTP , haga clic en el botón Enable	FTP : <input type="radio"/> Disable <input checked="" type="radio"/> Enable
Paso 8:	Escriba la dirección IP del servidor FTP	IP/Prefix length : <input type="text"/> / <input type="text"/>
Paso 9:	En Samba , haga clic en el botón Enable	Samba : <input type="radio"/> Disable <input checked="" type="radio"/> Enable
Paso 10:	Escriba la dirección IP del servidor Samba	IP/Prefix length : <input type="text"/> / <input type="text"/>
Paso 11:	Habilite ICMP	ICMP(Ping) : <input type="radio"/> Disable <input checked="" type="radio"/> Enable
Paso 12:	Escriba una dirección IP	IP/Prefix length : <input type="text" value="0.0.0.0"/> / <input type="text" value="0"/>

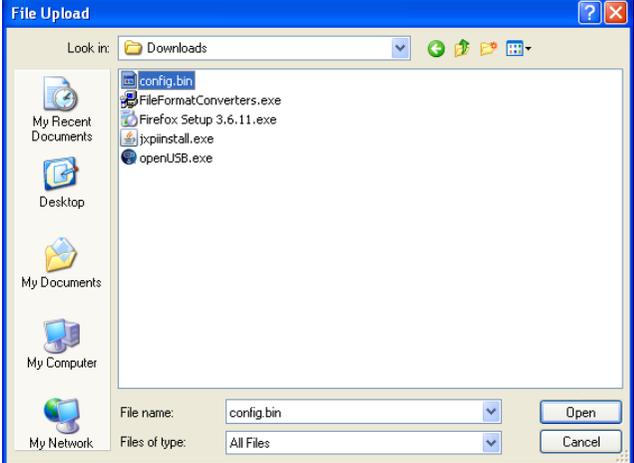
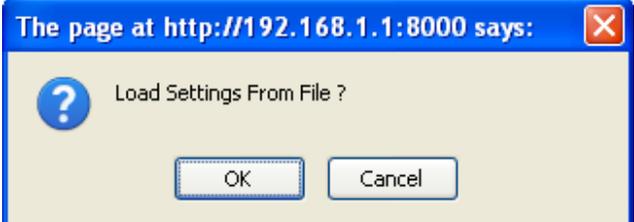
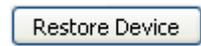
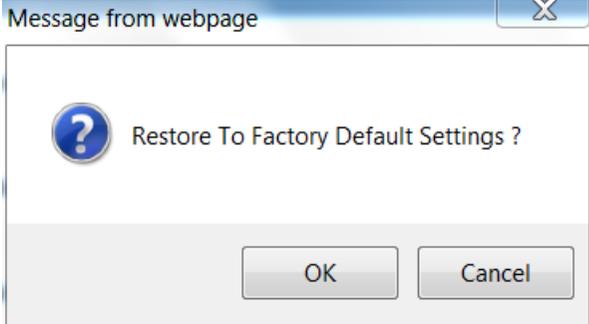
Capítulo 24: Trabajar con la configuración del sistema

Descripción general

La **Configuración del sistema** guarda todos sus ajustes automáticamente. Le permite reiniciar el router y/o restaurarlo a los valores por defecto de fábrica. Todos los ajustes del sistema pueden ser objeto de una copia de seguridad a través de la interfaz **Configuración del sistema**. Ahora vamos a ver con más detalle qué hay dentro de la ventana **Configuración del sistema**.

<p>Paso 1:</p>	<p>Abra el navegador y escriba la dirección IP por defecto del ASL-26555.</p>	
<p>Paso 2:</p>	<p>Escriba su Nombre de usuario y su Contraseña y haga clic en Log In.</p>	
<p>Paso 3:</p>	<p>Haga clic en Maintenance, System Settings (Configuración del sistema)</p>	
<p>Paso 4:</p>	<p>En Configuración del sistema hay dos ventanas</p> <ol style="list-style-type: none"> 1. La primera ventana es la descripción 2. La segunda ventana corresponde a los ajustes del sistema 	

<p>Paso 5:</p>	<p>Para Guardar y reiniciar el dispositivo, haga clic en el botón Reboot (Reiniciar)</p>	
<p>Paso 6:</p>	<p>Para Guardar ajustes en la unidad local, haga clic en el botón Save (Guardar)</p>	
<p>Paso 7:</p>	<p>Una ventana le pedirá que guarde el archivo localmente. Haga clic en Save File (Guardar archivo) y en OK</p>	
<p>Paso 8:</p>	<p>El archivo se guardará en su disco duro local</p>	
<p>Paso 9:</p>	<p>Para Guardar ajustes desde el disco duro local, haga clic en Explorar</p>	

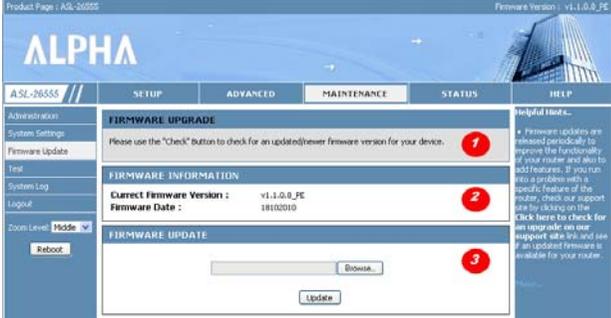
<p>Paso 10:</p>	<p>Localice el archivo en su ordenador</p>	
<p>Paso 11:</p>	<p>Haga clic en OK para guardar los ajustes desde el archivo</p>	
<p>Paso 12:</p>	<p>Para Restaurar los valores por defecto de fábrica, haga clic en Restaurar dispositivo</p>	
<p>Paso 13:</p>	<p>Aparecerá la ventana Mensaje desde la página web que le pedirá que verifique que desea Restaurar a los valores por defecto de fábrica. Haga clic en OK.</p>	

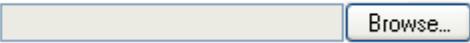
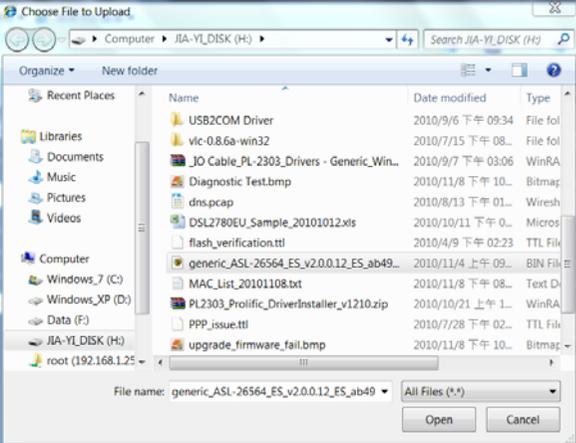
<p>Paso 14:</p>	<p>Aparecerá la ventana Configuración completa para confirmar que se han ajustado los valores por defecto de fábrica. Espere a que se reinicie el dispositivo.</p>		
------------------------	---	---	--

Capítulo 25: Trabajar con actualizaciones de firmware

Descripción general

La función Actualización de firmware del ASL-26555 es muy fácil de usar. Vamos a ver ahora con más detalle que hay dentro de la ventana **Firmware**.

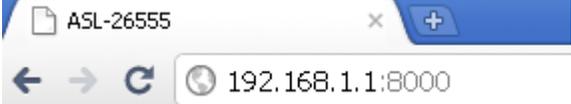
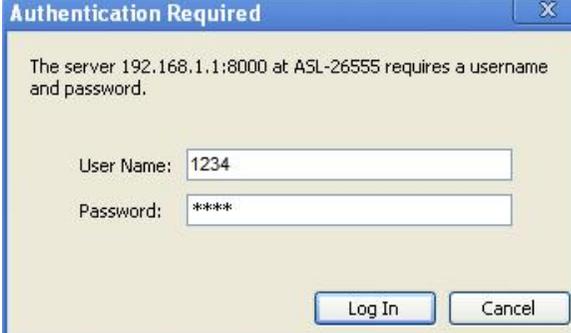
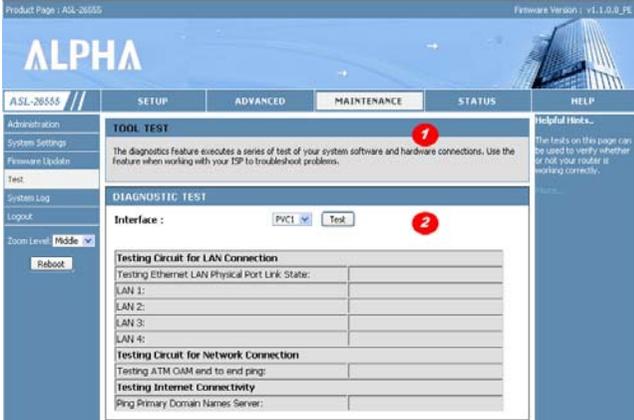
Paso 1:	Abra el navegador y escriba la dirección IP por defecto del ASL-26555.	
Paso 2:	Escriba su Nombre de usuario y su Contraseña y haga clic en Log In .	
Paso 3:	Haga clic en Maintenance, Firmware Update (Actualización de firmware)	
Paso 4:	En Actualización de firmware hay tres ventanas: 1. La primera ventana es la descripción 2. La segunda ventana es la Información de firmware 3. La tercera ventana es el cuadro Actualización de firmware	
Paso 5:	La segunda ventana ofrece Información sobre el firmware.	

<p>Paso 6:</p>	<p>En Actualización de firmware, haga clic en el botón Explorar para buscar el firmware</p>	
<p>Paso 7:</p>	<p>Seleccione la versión de firmware de su ordenador y haga clic en Abrir.</p>	
<p>Paso 8:</p>	<p>En el campo reservado a tal efecto aparecerá la versión de firmware seleccionada, haga clic en Actualizar</p>	
<p>Paso 9:</p>	<p>Cuando se haya verificado el firmware, aparecerá una ventana notificándole que su sistema se está reiniciando</p>	
	<p>IMPORTANTE: Si el archivo está corrupto o si no es el archivo correcto, aparecerá un mensaje de error.</p>	

Capítulo 26: Prueba de los ajustes

Descripción general

El ASL-26555 ofrece a los usuarios funciones de prueba. La herramienta de diagnóstico ofrece información sobre tantas interfaces como haya configurado el usuario. Prueba todos los puertos LAN, la actividad de la red y la conectividad a Internet. Ahora vamos a ver más de cerca que hay en la ventana **Probar**.

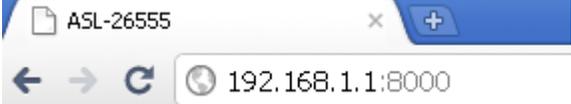
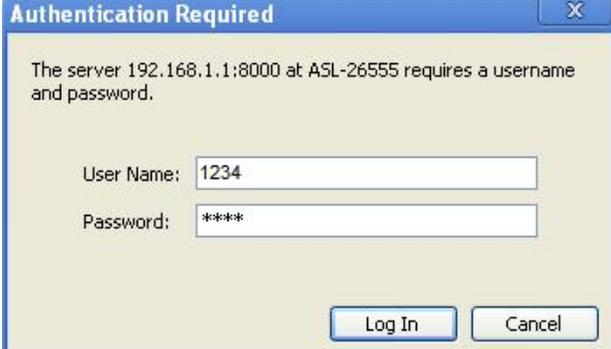
<p>Paso 1:</p>	<p>Abra el navegador y escriba la dirección IP por defecto del ASL-26555.</p>	
<p>Paso 2:</p>	<p>Escriba su Nombre de usuario y su Contraseña y haga clic en Log In.</p>	
<p>Paso 3:</p>	<p>Haga clic en Maintenance, Test</p>	
<p>Paso 4:</p>	<p>En Test hay dos ventanas:</p> <ol style="list-style-type: none"> 1. La primera ventana es la descripción 2. La segunda ventana es la prueba diagnóstica 	

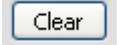
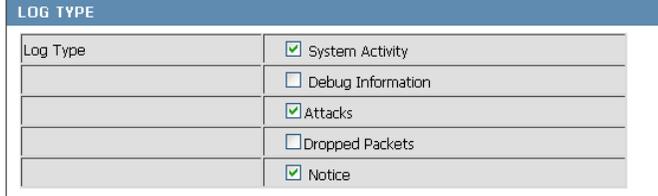
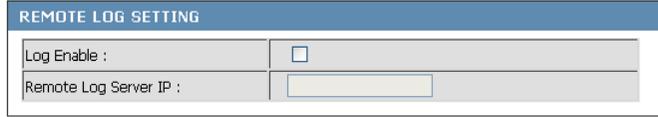
<p>Paso 5:</p>	<p>Para realizar una prueba diagnóstica, seleccione la interfaz y haga clic en Test</p>	<p>Interface : PVC1 Test</p>														
<p>Paso 6:</p>	<p>La tabla que aparece en la ventana de la prueba diagnóstica está en blanco antes de la prueba</p>	<p>Testing Circuit for LAN Connection</p> <table border="1"> <tr><td>Testing Ethernet LAN Physical Port Link State:</td><td></td></tr> <tr><td>LAN 1:</td><td></td></tr> <tr><td>LAN 2:</td><td></td></tr> <tr><td>LAN 3:</td><td></td></tr> <tr><td>LAN 4:</td><td></td></tr> </table> <p>Testing Circuit for Network Connection</p> <table border="1"> <tr><td>Testing ATM OAM end to end ping:</td><td></td></tr> </table> <p>Testing Internet Connectivity</p> <table border="1"> <tr><td>Ping Primary Domain Names Server:</td><td></td></tr> </table>	Testing Ethernet LAN Physical Port Link State:		LAN 1:		LAN 2:		LAN 3:		LAN 4:		Testing ATM OAM end to end ping:		Ping Primary Domain Names Server:	
Testing Ethernet LAN Physical Port Link State:																
LAN 1:																
LAN 2:																
LAN 3:																
LAN 4:																
Testing ATM OAM end to end ping:																
Ping Primary Domain Names Server:																
<p>Paso 7:</p>	<p>Si hace clic en el botón Test aparecerá un informe de progreso</p>	<p>DIAGNOSTIC TEST</p> <p>Interface : PVC1 Test</p> <p>Testing Circuit for LAN Connection</p> <table border="1"> <tr><td>Testing Ethernet LAN Physical Port Link State:</td><td>Progress...</td></tr> </table> <p>Testing Circuit for Network Connection</p> <table border="1"> <tr><td>Testing ATM OAM end to end ping:</td><td>Progress...</td></tr> </table> <p>Testing Internet Connectivity</p> <table border="1"> <tr><td>Ping Primary Domain Names Server:</td><td>Progress...</td></tr> </table>	Testing Ethernet LAN Physical Port Link State:	Progress...	Testing ATM OAM end to end ping:	Progress...	Ping Primary Domain Names Server:	Progress...								
Testing Ethernet LAN Physical Port Link State:	Progress...															
Testing ATM OAM end to end ping:	Progress...															
Ping Primary Domain Names Server:	Progress...															
<p>Paso 8:</p>	<p>Cuando se haya elaborado el informe de progreso, aparecerá un conjunto de resultados en la pantalla confirmando el final de la prueba diagnóstica</p> <p> IMPORTANTE: La información suministrada es una simple orientación para demostrarle que está funcionando y que no está en la red. Utilice aplicaciones terceras para obtener unos resultados diagnósticos completo.</p>	<p>DIAGNOSTIC TEST</p> <p>Interface : PVC1 Test</p> <p>Testing Circuit for LAN Connection</p> <table border="1"> <tr><td>Testing Ethernet LAN Physical Port Link State:</td><td>Success</td></tr> <tr><td>LAN 1:</td><td>Down</td></tr> <tr><td>LAN 2:</td><td>Up</td></tr> <tr><td>LAN 3:</td><td>Down</td></tr> <tr><td>LAN 4:</td><td>Down</td></tr> </table> <p>Testing Circuit for Network Connection</p> <table border="1"> <tr><td>Testing ATM OAM end to end ping:</td><td>Fail</td></tr> </table> <p>Testing Internet Connectivity</p> <table border="1"> <tr><td>Ping Primary Domain Names Server:</td><td>Fail</td></tr> </table>	Testing Ethernet LAN Physical Port Link State:	Success	LAN 1:	Down	LAN 2:	Up	LAN 3:	Down	LAN 4:	Down	Testing ATM OAM end to end ping:	Fail	Ping Primary Domain Names Server:	Fail
Testing Ethernet LAN Physical Port Link State:	Success															
LAN 1:	Down															
LAN 2:	Up															
LAN 3:	Down															
LAN 4:	Down															
Testing ATM OAM end to end ping:	Fail															
Ping Primary Domain Names Server:	Fail															

Capítulo 27: Comprender el registro de sistema

Descripción general

El ASL-26555 ofrece a los usuarios un Registro de sistema. El Registro de sistema permite a los usuarios guardar archivos de registro, borrar la lista de Registro y registrar distintas actividades en el ASL-26555. También existe la posibilidad de registrar actividades a distancia a través de un servidor de registro remoto. Ahora vamos a ver con más detalle que hay dentro de la ventana **Registro de sistema**.

Paso 1:	Abra el navegador y escriba la dirección IP por defecto del ASL-26555.	
Paso 2:	Escriba su Nombre de usuario y su Contraseña y haga clic en Log In .	
Paso 3:	Haga clic en Maintenance, System Log (Registro de sistema)	

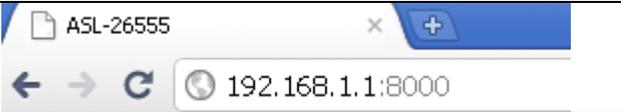
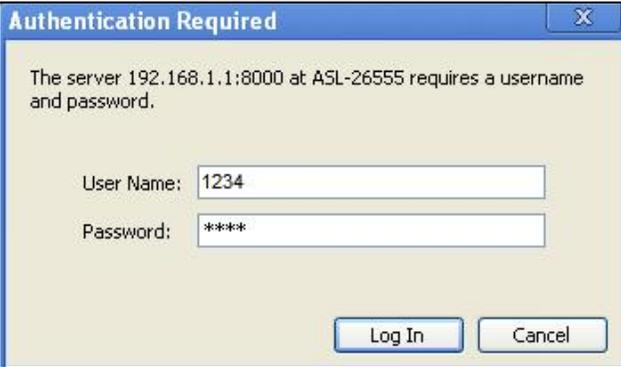
<p>Paso 4:</p>	<p>En Registro de sistema hay cuatro ventanas:</p> <ol style="list-style-type: none"> 1. La primera ventana es la descripción 2. La segunda ventana es el archivo Guardar registro 3. La tercera ventana es el Tipo de registro 4. La cuarta ventana corresponde a los Ajustes del registro remoto 	
<p>Paso 5:</p>	<p>Para guardar el archivo de registro, haga clic en Guardar y luego en Guardar archivo de registro en el disco duro local</p>	
<p>Paso 6:</p>	<p>Para borrar la Información de registro, haga clic en el botón Borrar</p>	
<p>Paso 7:</p>	<p>Para generar registros de determinadas actividades, marque la casilla de verificación junto al elemento que desea controlar</p>	
<p>Paso 8:</p>	<p>Para habilitar los registros remotos, marque la casilla de verificación Registro habilitado y escriba el IP del servidor del registro remoto</p>	
<p>Paso 9:</p>	<p>Haga clic en Add/Apply cuando haya terminado</p>	

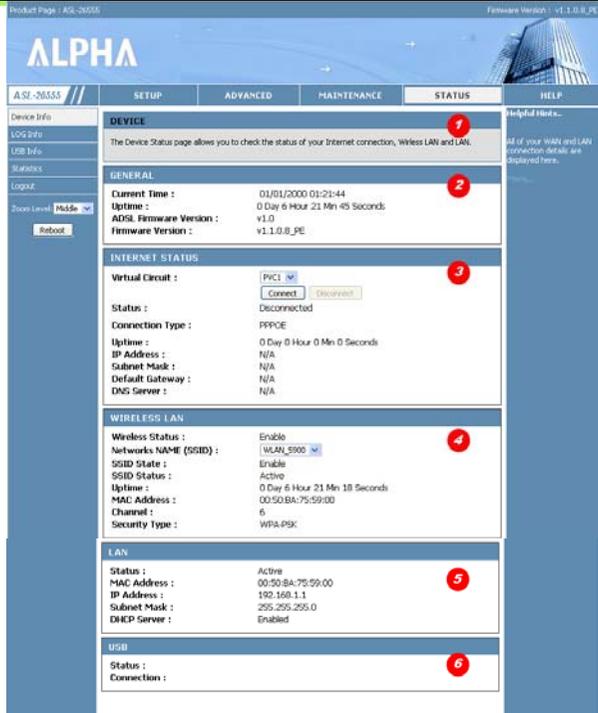
Capítulo 28: Comprender los informes de estado

Descripción general

El ASL-26555 ofrece a los usuarios un Informe de estado de los dispositivos y puertos. También ofrece estadísticas sobre la actividad de la red inalámbrica y las redes LAN/WAN. Veamos ahora qué hay en la ventana **Estado**. La primera ventana corresponde a la información sobre el dispositivo.

Información sobre el dispositivo

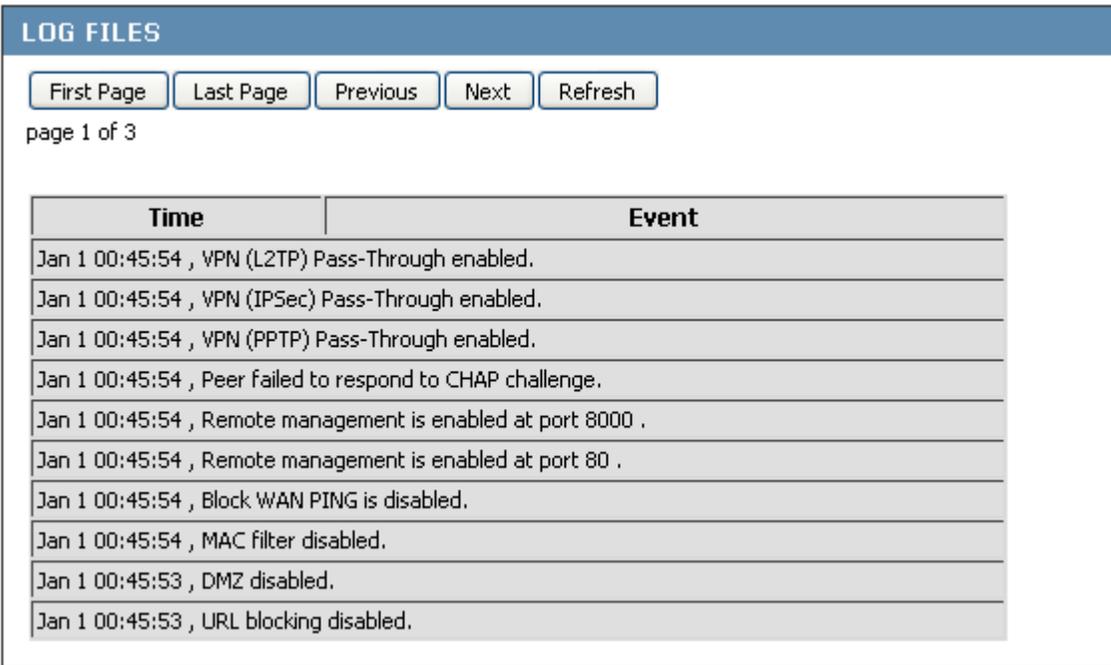
Paso 1:	Abra el navegador y escriba la dirección IP por defecto del ASL-26555.	
Paso 2:	Escriba su Nombre de usuario y su Contraseña y haga clic en Log In .	
Paso 3:	Haga clic en Status, Device Info (Información sobre el dispositivo)	

<p>Paso 4:</p>	<p>En Información sobre el dispositivo hay seis ventanas:</p> <ol style="list-style-type: none"> 1. La primera ventana es la descripción 2. La segunda ventana es el cuadro General 3. La tercera ventana es el cuadro Estado de Internet 4. La cuarta ventana es le cuadro LAN inalámbrica 5. La quinta ventana es el cuadro LAN 6. La sexta ventana es el cuadro USB 	 <p>The screenshot shows the ALPHA router's status page. It has a navigation menu with 'STATUS' selected. The main content area is divided into several sections: 'DEVICE' (1), 'GENERAL' (2), 'INTERNET STATUS' (3), 'WIRELESS LAN' (4), 'LAN' (5), and 'USB' (6). Each section contains specific status information and configuration options.</p>
<p>Paso 5:</p>	<p>El cuadro Dispositivo contiene una descripción de la Información sobre el dispositivo</p>	<p>DEVICE</p> <p>The Device Status page allows you to check the status of your Internet connection, Wireless LAN and LAN.</p>
<p>Paso 6:</p>	<p>El cuadro General contiene la hora actual, el tiempo de actividad, la versión del firmware ADSL y la versión del firmware completo</p>	<p>GENERAL</p> <p>Current Time : 01/01/2000 01:21:44 Uptime : 0 Day 6 Hour 21 Min 45 Seconds ADSL Firmware Version : v1.0 Firmware Version : v1.1.0.8_PE</p>

<p>Paso 7:</p>	<p>El cuadro Estado de Internet contiene el circuito virtual, el estado de Internet, el tipo de conexión, el tiempo de actividad, la dirección IP, la máscara de subred, la puerta de enlace por defecto y el servidor DNS</p>	<div style="background-color: #4F81BD; color: white; padding: 5px;">INTERNET STATUS</div> <p>Virtual Circuit : PVC1 <input type="button" value="Connect"/> <input type="button" value="Disconnect"/></p> <p>Status : Disconnected</p> <p>Connection Type : PPPOE</p> <p>Uptime : 0 Day 0 Hour 0 Min 0 Seconds</p> <p>IP Address : N/A</p> <p>Subnet Mask : N/A</p> <p>Default Gateway : N/A</p> <p>DNS Server : N/A</p>
<p>Paso 8:</p>	<p>El cuadro LAN inalámbrica ofrece información de estado sobre el estado inalámbrico, la SSID de la red (dentro de un entorno inalámbrico), el estado de la SSID, el tiempo de actividad, la dirección MAC, el canal de red y el tipo de seguridad</p>	<div style="background-color: #4F81BD; color: white; padding: 5px;">WIRELESS LAN</div> <p>Wireless Status : Enable</p> <p>Networks NAME (SSID) : WLAN_5900 <input type="button" value="v"/></p> <p>SSID State : Enable</p> <p>SSID Status : Active</p> <p>Uptime : 0 Day 6 Hour 21 Min 18 Seconds</p> <p>MAC Address : 00:50:BA:75:59:00</p> <p>Channel : 6</p> <p>Security Type : WPA-PSK</p>
<p>Paso 9:</p>	<p>El cuadro LAN ofrece informes de estado sobre la LAN, información sobre la dirección MAC, la dirección IP, la máscara de subred y el servidor DHCP</p>	<div style="background-color: #4F81BD; color: white; padding: 5px;">LAN</div> <p>Status : Active</p> <p>MAC Address : 00:50:BA:75:59:00</p> <p>IP Address : 192.168.1.1</p> <p>Subnet Mask : 255.255.255.0</p> <p>DHCP Server : Enabled</p>
<p>Paso 10:</p>	<p>El cuadro USB ofrece información sobre el estado USB y su conexión</p>	<div style="background-color: #4F81BD; color: white; padding: 5px;">USB</div> <p>Status :</p> <p>Connection :</p>

Información de registro

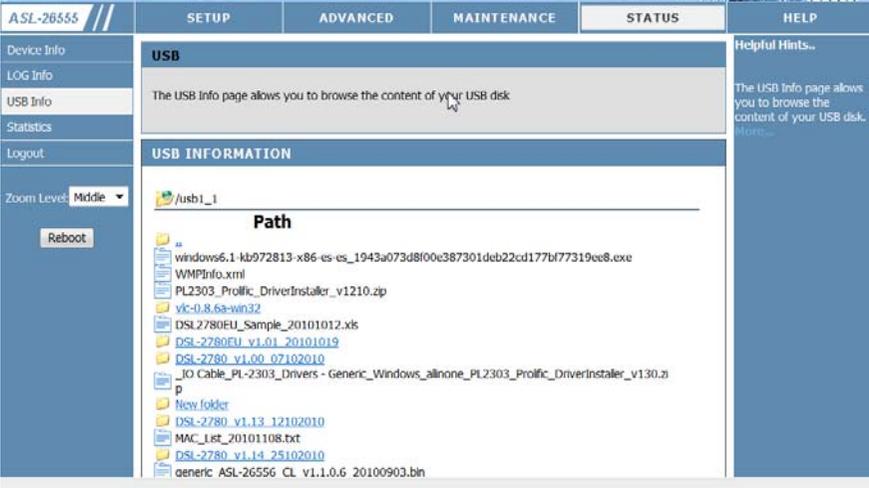
Paso 1:	Haga clic en Estado, Información de registro	<div style="border: 1px solid black; padding: 5px;"> <div style="display: flex; justify-content: space-between; border-bottom: 1px solid black;"> STATUS LOG Info </div> </div>
Paso 2:	<p>En Información de registro hay tres ventanas:</p> <ol style="list-style-type: none"> 1. La primera ventana es la descripción 2. La segunda ventana es el cuadro Servidor del registro 3. La tercera ventana es el cuadro Archivos de registro 	 <p>The screenshot shows the ALPHA web interface. At the top, there are tabs for SETUP, ADVANCED, MAINTENANCE, STATUS (selected), and HELP. The main content area is divided into three sections: SYSTEM LOG, LOG SERVER, and LOG FILES. Red circles with numbers 1, 2, and 3 highlight these sections respectively. The SYSTEM LOG section contains the text 'System Log stores internal system informations.'. The LOG SERVER section shows 'Log Server : Enable' and 'Log Server Address : 192.168.1.50'. The LOG FILES section shows a table of log entries with columns 'Time' and 'Event', and navigation buttons like 'First Page', 'Last Page', 'Previous', 'Next', and 'Refresh'. A 'Reboot' button is visible in the left sidebar.</p>
Paso 3:	El Registro del sistema es una descripción del registro del sistema	<div style="border: 1px solid black; padding: 5px;"> <div style="background-color: #4f81bd; color: white; padding: 5px;">SYSTEM LOG</div> <div style="background-color: #e0e0e0; padding: 5px;">System Log stores internal system informations.</div> </div>
Paso 4:	El Servidor del registro ofrece información sobre el Servidor del registro y la Dirección IP del servidor del registro	<div style="border: 1px solid black; padding: 5px;"> <div style="background-color: #4f81bd; color: white; padding: 5px;">LOG SERVER</div> <div style="padding: 5px;"> <p>Log Server : Enable</p> <p>Log Server Address : 192.168.1.50</p> </div> </div>

<p>Paso 5:</p>	<p>El cuadro Archivos de registro ofrece una tabla con distinta información sobre el protocolo, el filtro y el sistema interno. Los usuarios pueden explorar varias páginas de información sobre los archivos de registro</p>	 <p>The screenshot shows a web interface titled "LOG FILES". At the top, there are navigation buttons: "First Page", "Last Page", "Previous", "Next", and "Refresh". Below the buttons, it says "page 1 of 3". A table with two columns, "Time" and "Event", lists the following entries:</p> <table border="1"> <thead> <tr> <th>Time</th> <th>Event</th> </tr> </thead> <tbody> <tr> <td>Jan 1 00:45:54</td> <td>, VPN (L2TP) Pass-Through enabled.</td> </tr> <tr> <td>Jan 1 00:45:54</td> <td>, VPN (IPSec) Pass-Through enabled.</td> </tr> <tr> <td>Jan 1 00:45:54</td> <td>, VPN (PPTP) Pass-Through enabled.</td> </tr> <tr> <td>Jan 1 00:45:54</td> <td>, Peer failed to respond to CHAP challenge.</td> </tr> <tr> <td>Jan 1 00:45:54</td> <td>, Remote management is enabled at port 8000 .</td> </tr> <tr> <td>Jan 1 00:45:54</td> <td>, Remote management is enabled at port 80 .</td> </tr> <tr> <td>Jan 1 00:45:54</td> <td>, Block WAN PING is disabled.</td> </tr> <tr> <td>Jan 1 00:45:54</td> <td>, MAC filter disabled.</td> </tr> <tr> <td>Jan 1 00:45:53</td> <td>, DMZ disabled.</td> </tr> <tr> <td>Jan 1 00:45:53</td> <td>, URL blocking disabled.</td> </tr> </tbody> </table>	Time	Event	Jan 1 00:45:54	, VPN (L2TP) Pass-Through enabled.	Jan 1 00:45:54	, VPN (IPSec) Pass-Through enabled.	Jan 1 00:45:54	, VPN (PPTP) Pass-Through enabled.	Jan 1 00:45:54	, Peer failed to respond to CHAP challenge.	Jan 1 00:45:54	, Remote management is enabled at port 8000 .	Jan 1 00:45:54	, Remote management is enabled at port 80 .	Jan 1 00:45:54	, Block WAN PING is disabled.	Jan 1 00:45:54	, MAC filter disabled.	Jan 1 00:45:53	, DMZ disabled.	Jan 1 00:45:53	, URL blocking disabled.
Time	Event																							
Jan 1 00:45:54	, VPN (L2TP) Pass-Through enabled.																							
Jan 1 00:45:54	, VPN (IPSec) Pass-Through enabled.																							
Jan 1 00:45:54	, VPN (PPTP) Pass-Through enabled.																							
Jan 1 00:45:54	, Peer failed to respond to CHAP challenge.																							
Jan 1 00:45:54	, Remote management is enabled at port 8000 .																							
Jan 1 00:45:54	, Remote management is enabled at port 80 .																							
Jan 1 00:45:54	, Block WAN PING is disabled.																							
Jan 1 00:45:54	, MAC filter disabled.																							
Jan 1 00:45:53	, DMZ disabled.																							
Jan 1 00:45:53	, URL blocking disabled.																							

Información USB

<p>Paso 1:</p>	<p>Haga clic en Status, USB Info (Información USB)</p>	 <p>The screenshot shows two buttons: "STATUS" and "USB Info". The "STATUS" button is highlighted with a blue border.</p>
-----------------------	---	--

<p>Paso 2:</p>	<p>En Información USB hay dos ventanas:</p> <ol style="list-style-type: none"> 1. La primera ventana es la descripción 2. La segunda ventana es el cuadro Información USB 	
<p>Paso 3:</p>	<p>Conecte un dispositivo USB al ASL-26555 para recibir información sobre su contenido.</p> <p> IMPORTANTE: Si se conecta un dispositivo USB al ASL-26555, en la pestaña Información sobre el dispositivo, el indicador de estado USB señalará que el dispositivo está conectado mostrando Activo cuando esté conectado e Inactivo cuando esté desconectado.</p>	

<p>Paso 4:</p>	<p>En el caso de los dispositivos USB conectados, la ventana INFORMACIÓN USB mostrará el directorio de archivos USB</p>	
<p>Paso 5:</p>	<p>Si hay una impresora conectada al ASL-26555, aparecerá un icono en forma de impresora</p>	
<p>Paso 6:</p>	<p>Si hay un adaptador USB 3G conectada al ASL-26555, aparecerá un icono 3G</p>	

Estadísticas

<p>Paso 1:</p>	<p>Haga clic en Status, Statistics (Estadísticas)</p>	
-----------------------	--	---

Paso 2: En **Estadísticas** hay tres ventanas:

1. La primera ventana corresponde a las Estadísticas de tráfico
2. La segunda ventana es el cuadro estadístico para la conectividad inalámbrica, LAN y WAN
3. La tercera ventana ofrece estadísticas ADSL

Product Page : ASL-26555 Firmware Version : v1.1.0.8_PE

ALPHA

ASL-26555 // SETUP ADVANCED MAINTENANCE STATUS HELP

Device Info
LOG Info
USB Info
Statistics
Logout

Zoom Level: Middle
Reboot

TRAFFIC STATISTICS 1

Traffic Statistics display Receive and Transmit packets passing through the Device.

Refresh

STATISTICS 2

Interface	Transmit				Receive			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
LAN:	354243	451	0	0	58681	580	0	0
WAN: PVC1	0	0	0	0	0	0	0	0
Wireless: WLAN_5900	0	199	0	0	3206218	21323	0	0

ADSL STATISTICS 3

ADSL Mode	Auto Sync-Up	
ADSL Type	Annex A	
Status	Down	
	Downstream	Upstream
Rate(Kbps)	0	0
SNR Margin(dB)	0	0
Attenuation(dB)	0	0
Output Power(dBm)	0	0
Super Frames	0	0
RS Correctable Errors	0	0
RS Uncorrectable Errors	0	0
HEC Errors	0	0
Total Cells	0	0
Data Cells	0	0
Bit Errors	0	0

Helpful Hints..
This is a summary of the number of packets that have passed between the WAN and the LAN since the router was last initialized.
More...

Paso 3: En **Estadísticas de tráfico**, haga clic en **Actualizar** para obtener las últimas estadísticas acerca del ASL-26555

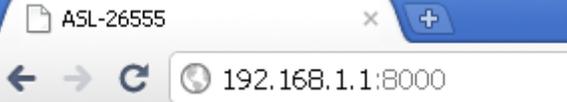
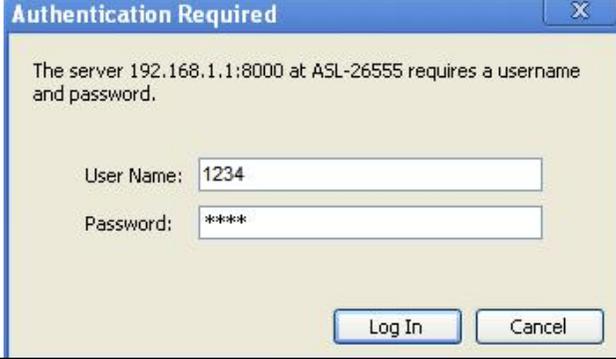
Refresh

<p>Paso 4:</p>	<p>En Estadísticas, las tres interfaces (LAN/WAN/inalámbrica) publican información sobre los datos recibidos y transmitidos. Muestra datos sobre los paquetes, errores, paquetes caídos y tamaños de byte generales.</p>	<table border="1"> <thead> <tr> <th colspan="9">STATISTICS</th> </tr> <tr> <th rowspan="2">Interface</th> <th colspan="4">Transmit</th> <th colspan="4">Receive</th> </tr> <tr> <th>Bytes</th> <th>Pkts</th> <th>Errs</th> <th>Drops</th> <th>Bytes</th> <th>Pkts</th> <th>Errs</th> <th>Drops</th> </tr> </thead> <tbody> <tr> <td>LAN:</td> <td>354243</td> <td>451</td> <td>0</td> <td>0</td> <td>58681</td> <td>580</td> <td>0</td> <td>0</td> </tr> <tr> <td>WAN: <input type="button" value="▼"/></td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> <tr> <td>Wireless: <input type="button" value="▼"/></td> <td>0</td> <td>199</td> <td>0</td> <td>0</td> <td>3206218</td> <td>21323</td> <td>0</td> <td>0</td> </tr> </tbody> </table>	STATISTICS									Interface	Transmit				Receive				Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops	LAN:	354243	451	0	0	58681	580	0	0	WAN: <input type="button" value="▼"/>	0	0	0	0	0	0	0	0	Wireless: <input type="button" value="▼"/>	0	199	0	0	3206218	21323	0	0							
STATISTICS																																																														
Interface	Transmit				Receive																																																									
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops																																																						
LAN:	354243	451	0	0	58681	580	0	0																																																						
WAN: <input type="button" value="▼"/>	0	0	0	0	0	0	0	0																																																						
Wireless: <input type="button" value="▼"/>	0	199	0	0	3206218	21323	0	0																																																						
<p>Paso 5:</p>	<p>En Estadísticas ADSL, toda la información se refiere a su Modo, Tipo y Estado. Los datos publicados revelan información de subida y de bajada sobre las distintas funciones del ASL-26555.</p>	<table border="1"> <thead> <tr> <th colspan="3">ADSL STATISTICS</th> </tr> </thead> <tbody> <tr> <td>ADSL Mode</td> <td colspan="2">Auto Sync-Up</td> </tr> <tr> <td>ADSL Type</td> <td colspan="2">Annex A</td> </tr> <tr> <td>Status</td> <td colspan="2">Down</td> </tr> <tr> <td></td> <td></td> <td></td> </tr> <tr> <td></td> <td>Downstream</td> <td>Upstream</td> </tr> <tr> <td>Rate(Kbps)</td> <td>0</td> <td>0</td> </tr> <tr> <td></td> <td></td> <td></td> </tr> <tr> <td>SNR Margin(dB)</td> <td>0</td> <td>0</td> </tr> <tr> <td>Attenuation(dB)</td> <td>0</td> <td>0</td> </tr> <tr> <td>Output Power(dBm)</td> <td>0</td> <td>0</td> </tr> <tr> <td></td> <td></td> <td></td> </tr> <tr> <td>Super Frames</td> <td>0</td> <td>0</td> </tr> <tr> <td>RS Correctable Errors</td> <td>0</td> <td>0</td> </tr> <tr> <td>RS Uncorrectable Errors</td> <td>0</td> <td>0</td> </tr> <tr> <td></td> <td></td> <td></td> </tr> <tr> <td>HEC Errors</td> <td>0</td> <td>0</td> </tr> <tr> <td>Total Cells</td> <td>0</td> <td>0</td> </tr> <tr> <td>Data Cells</td> <td>0</td> <td>0</td> </tr> <tr> <td>Bit Errors</td> <td>0</td> <td>0</td> </tr> </tbody> </table>	ADSL STATISTICS			ADSL Mode	Auto Sync-Up		ADSL Type	Annex A		Status	Down						Downstream	Upstream	Rate(Kbps)	0	0				SNR Margin(dB)	0	0	Attenuation(dB)	0	0	Output Power(dBm)	0	0				Super Frames	0	0	RS Correctable Errors	0	0	RS Uncorrectable Errors	0	0				HEC Errors	0	0	Total Cells	0	0	Data Cells	0	0	Bit Errors	0	0
ADSL STATISTICS																																																														
ADSL Mode	Auto Sync-Up																																																													
ADSL Type	Annex A																																																													
Status	Down																																																													
	Downstream	Upstream																																																												
Rate(Kbps)	0	0																																																												
SNR Margin(dB)	0	0																																																												
Attenuation(dB)	0	0																																																												
Output Power(dBm)	0	0																																																												
Super Frames	0	0																																																												
RS Correctable Errors	0	0																																																												
RS Uncorrectable Errors	0	0																																																												
HEC Errors	0	0																																																												
Total Cells	0	0																																																												
Data Cells	0	0																																																												
Bit Errors	0	0																																																												

Capítulo 29: Obtener ayuda con la Ayuda

Descripción general

El ASL-26555 ofrece a los usuarios un completo menú de Ayuda. El menú de Ayuda trata temas que cubren las principales funciones del router. La sección Ayuda está dividida en cinco secciones con sus propias explicaciones. Vamos a ver ahora más de cerca qué hay en la ventana **Ayuda**.

Paso 1:	Abra el navegador y escriba la dirección IP por defecto del ASL-26555.	
Paso 2:	Escriba su Nombre de usuario y su Contraseña y haga clic en Log In .	
Paso 3:	Haga clic en Help (Ayuda)	

Sigue una lista de los elementos en cada menú de ayuda:

- Paso 1:** En **Menú** hay cinco ventanas:
1. La primera ventana es el índice de la **Ayuda**
 2. La segunda ventana es el índice de la **Ayuda de configuración**
 3. La tercera ventana es el índice de la **Ayuda avanzada**
 4. La cuarta ventana es el índice de la **Ayuda de mantenimiento**
 5. La quinta ventana es el índice de la **Ayuda de estado**

Product Page : ASL-26555 Firmware Version : v1.1.0.8_PE

ALPHA

ASL-26555 // SETUP ADVANCED MAINTENANCE STATUS HELP

Menu
Setup
Advanced
Maintenance
Status
Logout
Zoom Level: Middle
Reboot

HELP SETUP

- Setup
- Advanced
- Maintenance
- Status

SETUP HELP

- Wizard
- Internet Setup
- Local Network
- Time and Date

ADVANCED HELP

- DNS
- Dynamic Dns
- Applications
- Filter
- Parental Control
- Firewall
- Virtual Server
- QoS
- Routing
- DMZ (Exposed Host)
- RIP
- IGMP
- PortMap
- AddrMap
- DHCP
- UPnP
- TR069
- Samba
- Wireless Setup
- WLAN Access Rules
- Multiple WLAN SSIDs
- WLAN Performance
- SNMP

MAINTENANCE HELP

- Administration
- System Settings
- Firmware Update
- Test
- System Log

STATUS HELP

- Device Info
- LOG Info
- USB Info
- Statistics

BROADBAND

Copyright © 2004-2010 Systems, Inc.

En **Configuración** hay cinco ventanas:

1. La primera ventana es el índice de **Configuración**
2. La ventana dos es el **Asistente**
3. La tercera ventana es la **Configuración de Internet**
4. La cuarta ventana es la **Red local**
5. La quinta ventana corresponde a la **Hora y Fecha**

Product Page : ASL-26555 Firmware Version : v2.0.0.33B_ES

ALPHA

ASL-26555 // SETUP ADVANCED MAINTENANCE STATUS HELP

Menu
Setup
Advanced
Maintenance
Status
Logout

Zoom Level: Middle

Reboot

SETUP

- [Wizard](#)
- [Internet Setup](#)
- [Local Network](#)
- [Time and Date](#)

WIZARD

Setup Wizard

The Setup Wizard is a useful and easy utility to help setup the device to quickly connect to your ISP (Internet Service Provider) with only a few steps required. It will guide you step by step to configure time zone, and WAN settings of your device. The Setup Wizard is a helpful guide for first time users to the device.

[Top](#)

INTERNET SETUP

ADSL SETTING

ADSL setting allows the user to set the configuration for ADSL protocols.

ATM VC SETTING

ATM VC Setting are settings that are used to connect to your ISP. These settings may be referred to as Public settings. Your ISP provides these settings to you. Please select the appropriate option to connect to your ISP.

Interface

Select which interface will be setup.

Enable Virtual Circuit

Enable or Disable this VC. The VC identifies the physical path the data takes to reach your ISP.

VPI

If instructed to change this, type in the VPI value for the initial connection (using PVC1). Default= 8.

VCI

If instructed to change this, type in the VCI value for the initial connection (using PVC1). Default= 35.

Service Category

Select the ATM service category.

PCR

Leave the setting at the default value 0 the first time the Router is set up. Enter the ATM PCR value.

WAN Settings

WAN Settings are settings that are used to connect to your ISP. These settings may be referred to as Public

LOCAL NETWORK

LAN Settings 4

These are the IP settings of the LAN interface for the device. These settings may be referred to as Private settings. You may change the LAN IP address if needed. The LAN IP address is private to your internal network and cannot be seen on the Internet. The default IP address is 192.168.15.1 with a subnet mask of 255.255.255.0. You may enter a local domain name for the LAN network if you prefer.

DHCP Server

DHCP stands for Dynamic Host Control Protocol. The DHCP server gives out IP addresses when a device is booting up and request an IP address to be logged on to the network. That device must be set as a DHCP client to "Obtain the IP address automatically". By default, the DHCP Server is enabled. The DHCP address pool contains the range of the IP address that will automatically be assigned to the clients on the network.

Starting IP address

The starting IP address for the DHCP server's IP assignment.

Ending IP address

The ending IP address for the DHCP server's IP assignment.

DHCP Reservations

DHCP Reservations List is a list of clients with a pairing of IP address and MAC address. The DHCP server will reserve these IP addresses for these clients in whatever situation if the list was enabled.

DHCP Clients List

DHCP client computers will have their information displayed in the Client Table. The Client Table will show the Host Name, IP Address, and MAC Address of each client computer.

[Top](#)

TIME AND DATE

Automatic Time Configuration 5

Select this option if you want to synchronize the router's clock to a Network Time Server over the Internet. If you are using schedules or logs, this is the best way to ensure that the schedules and logs are kept accurate.

NTP Server Used

Select a Network Time Server for synchronization. You can type in the address of a time server or select one from the list. If you have trouble using one server, select another.

Time Zone

Select your local time zone from pull down menu.

[Top](#)

En **Avanzado** hay veinticuatro ventanas:

1. La primera es el índice de **Avanzado**
2. La segunda corresponde a **DNS**
3. La tercera corresponde a **DNS dinámico**
4. La cuarta es **Aplicaciones**
5. La quinta es **Filtro**
6. La sexta es **Control parental**
7. La séptima es **Cortafuegos**
8. La octava es **Servidor virtual**
9. La novena es **Calidad de Servicio**
10. La décima es **Enrutamiento**
11. La decimoprimer es **DMZ (host expuesto)**
12. La decimosegunda es **RIP**
13. La decimotercera es **IGMP**
14. La decimocuarta es **Portmap**
15. La decimoquinta es **AddrMap**
16. La decimosexta es **DHCP**
17. La decimoséptima es **UPNP**
18. La decimooctava es **TR069**
19. La decimonovena es **SAMBA**
20. La vigésima es **Configuración inalámbrica**
21. La vigesimoprimer es la **Regla de acceso WLAN**
22. La vigesimosegunda es **SSID WLAN múltiples**
23. La vigesimotercera es **Rendimiento WLAN**
24. La vigesimocuarta es **SNMP**

The screenshot shows the web interface for the ASL-26555 router. At the top, it displays 'Product Page : ASL-26555' and 'Firmware Version : v2.0.0.33B_ES'. The main header features the 'ALPHA' logo and navigation tabs for 'ASL-26555 //', 'SETUP', 'ADVANCED', 'MAINTENANCE', 'STATUS', and 'HELP'. A left sidebar contains a 'Menu' with options: 'Setup', 'Advanced', 'Maintenance', 'Status', 'Logout', and 'Zoom Level: Middle'. A 'Reboot' button is also present. The main content area is titled 'ADVANCED' and contains a list of links: DNS, Dynamic Dns, Applications, Filter, Parental Control, Firewall, Virtual Server, QoS, Routing, DMZ (Exposed Host), RIP, IGMP, PortMap, AddrMap, DHCP, UPnP, TR069, Samba, Wireless Setup, WLAN Access Rules, Multiple WLAN SSIDs, WLAN Performance, and SNMP. Below this list are three sections: 'DNS' (with a red circle '1' highlighting the list), 'DNS' (with a red circle '2' highlighting the text), and 'DYNAMIC DNS' (with a red circle '3' highlighting the text).

ADVANCED

- [DNS](#)
- [Dynamic Dns](#)
- [Applications](#)
- [Filter](#)
- [Parental Control](#)
- [Firewall](#)
- [Virtual Server](#)
- [QoS](#)
- [Routing](#)
- [DMZ \(Exposed Host\)](#)
- [RIP](#)
- [IGMP](#)
- [PortMap](#)
- [AddrMap](#)
- [DHCP](#)
- [UPnP](#)
- [TR069](#)
- [Samba](#)
- [Wireless Setup](#)
- [WLAN Access Rules](#)
- [Multiple WLAN SSIDs](#)
- [WLAN Performance](#)
- [SNMP](#)

DNS

If Obtain DNS server address automatically is selected, the Router will accept the dynamically assigned DNS assignment from one of the PPPoA, PPPoE or DHCP enabled PVC(s) during the establishment of the connection. If Use the following DNS server addresses is selected, enter the Preferred and optional Alternate DNS server IP addresses.

[Top](#)

DYNAMIC DNS

To use Dynamic DNS you have to register at a DDNS provider (dyndns.org (<http://www.dyndns.org>) or no-ip.com (<http://www.no-ip.com>)) beforehand.

With DDNS the dynamic IP address of your computer will be resolved to a permanent host name.

- Enable the "Dynamic DNS" option.
- Select the DNS Relay.
- In the "User name" field enter the user name for your DDNS account.
- In the "Password" and "Confirm Password" fields enter the password for your DDNS account.

APPLICATIONS

The Application allows you to do port forwarding, but only have the ports open when data is sent out of the trigger ports. When a program sends data out on outgoing ports called trigger ports, the device then allows incoming data on the open ports specified in your port triggering configuration.

4

Trigger Port Start

Specify the start port on the device that would trigger the device to open ports for incoming data.

Trigger Port End

Specify the end port on the device that would trigger the device to open ports for incoming data. You can enter a port number the same as the trigger port start or enter a larger port number to specify a port range.

Trigger Traffic Protocol Type
Select the trigger traffic type.

Open Port

Specify all the ports to be opened. It's content could be:

1. A single port only.
2. A port range only. Start open port number and end port number should be separated by "-".
3. Combined several single port and several port ranges. Each single port or port range should be separated by ",".

Open Traffic Protocol Type
Select the open traffic type.

[Top](#)

FILTER

IP Filters

5

Filters manage the LAN users' access to the Internet. It is possible to permit the access to the Internet for specified IP addresses within your LAN or to restrict the access for specified IP addresses. You can also define filters for the access to ports.

For filtering a single IP address, please enter the value into both fields (from/to).

For filtering a single Port, please enter the same value into both fields (from/to).

MAC Filters

MAC filter enables users to specify the desired source MAC address, destination MAC address and/or protocol.

PARENTAL CONTROL

Create a list of Websites URL that you would like the devices on your network to be a **6** denied access to. Keywords can be entered in this list in order to block any URL containing the keyword entered.

[Top](#)

FIREWALL

In computing, a firewall is a piece of hardware and/or software which functions in a network environment to prevent some communications forbidden by the security policy, analogous to the function of walls in building construction. **7**

A firewall has the basic task of controlling traffic between different zones of trust. Typical zones of trust include the Internet (a zone with no trust) and an internal network (a zone with high trust).

The ultimate goal is to provide controlled connectivity between zones of differing trust levels through the enforcement of a security policy and connectivity model based on the least privilege principle.

DoS Attacks

A denial-of-service attack (also, DoS attack) is an attack on a computer system or network that causes a loss of service to users, typically the loss of network connectivity and services by consuming the bandwidth of the victim network or overloading the computational resources of the victim system.

Port Scans

Port Scans are a favoured method to detect potential weak points in your LAN.

A Port Scanner tries to gather information about active services on a machine by connecting to a server (Connect Scan) or getting answer to invalid data packets (Stealth Scan).

Service Filtering

Using Service Filtering will deny answers of certain (internal) services to attacks form the outside.

[Top](#)

VIRTUAL SERVER

A Virtual Server is defined as service port. All requests to this port of your external IP address will be forwarded to a certain internal IP address, e.g. requests via FTP oder POP3. **8**

Use the Virtual Server to forward hack attacks via HTTP to your HTTP server in the DMZ.

Example

You want to set up one FTP server, one Web server and an VPN server for your LAN.

Add 3 new rules:

QoS

QoS function is only used with router mode PVC, bridge mode PVC is not supported now.

9

In "Traffic Classifier" page, four type of classifiers could be used to set the priority for different knids of upstream packet.

Classifiers could be used at the same time and classifier's priority will be: "User Defined" > "Application" > "TOS DSCP" > "TOS Precedence".

Packets could be classify to 5 types : "Highest(Realtime)" is the highest priority and "Best Effert" is the lowest priority.

Improves your VoIP voice quality or streaming by ensuring that your VoIP or streaming traffic is prioritized over other network traffic, such as FTP or Web.

In "IP QoS" page, each PVC could enable/disable QoS function individual.

Each PVC's maximum upstream data rate could be specified in "Bandwidth" field.

All packets belong to "Highest(Realtime)" priority will be treated by Strict Priority algorithm(SPQ).

It means that those type of packets will be send immediately.

Another 4 type of packet's priority("Higher", "High", "Normal" and "Best Effert") will be treated by Weighted Fair algorith(WFQ).

Each priority's weight could be specified in "Weight" field.

[Top](#)

ROUTING

Routing protocols specify the ways (routes) of data packets in your LAN and in the Internet. No all out-bound data packets from your LAN will be send via a gateway, e.g. the ASL-26555, to the serv ISP and into the internet accordingly.

10

As the internet is based on packet-switching protocols, the way for each data packet is determined on every network knot anew.

DMZ (EXPOSED HOST)

DMZ is short for Demilitarized Zone.

11

A demilitarized zone is a network area (a subnetwork) that sits between an your internal network and an external network, usually the Internet. The point of a DMZ is that connections from the internal and the external network to the DMZ are permitted, whereas connections from the DMZ are only permitted to the external network - hosts in the DMZ may not connect to the internal network. This allows the DMZ's hosts to provide services to the external network while protecting the internal network in case intruders compromise a host in the DMZ. For someone on the external network who wants to illegally connect to the internal network, the DMZ is a dead end.

The ASL-26555 uses a slightly different approach. The DMZ (Exposed Host) connects to the internal network without further security. That is, the DMZ host is able to connect to hosts on the internal network, but hosts in a real DMZ are prevented from doing so by the firewall that sits between them.

[Top](#)

RIP

The routing information protocol (RIP) is one of the most commonly used interior gateway protocol (IGP) routing protocols on internal networks (and to a lesser extent, networks connected to the Internet) which helps routers dynamically adapt to changes of network connections by communicating information about which networks each router can reach and how far away those networks are.

12

There is no need to activate this option normally.

[Top](#)

IGMP

With IGMP Proxy/Snooping enabled, the device (L2 switch) can make intelligent multicast flooding (only) toward those hosts, i.e. IPSTBs, etc., which request to join (as members of) a specific multicast group, i.e. an IPTV channel, etc., within the broadcast domain (same PVC/VLAN). As a result, it significantly reduces traffic flooding upon interfaces that are not registered as receivers of specific multicast groups.

13

[Top](#)

PORTMAP

PORTMAP is used to allow PVC and LAN mapping .

14

[Top](#)

ADDRMAP

AddrMap is used to allow PVC mapping .

15

[Top](#)

DHCP

DHCP short for: Dynamic Host Configuration Protocol.

16

This protocol serves for the dynamic configuration of IP addresses and related information.

			<p>UPNP</p> <p>UPnP short for Universal Plug and Play is based on a series on standard network protocols and ports. Via UPnP various device, e.g. stereo system, router, printer, can be controlled manufacturer specific over an IP based network.</p> <p>Top</p>	
			<p>TR069</p> <p>TR-069 (short for Technical Report 069) defines an application layer protocol for remote management of end-user devices. It provides the communication between CPE and Auto Configuration Servers (ACS). ASL-26555 can get in contact with the Auto Configuration Servers (ACS) and establish the configuration automatically by TR-069.</p> <p>Top</p>	
			<p>SAMBA</p> <p>Samba.</p> <p>Top</p>	
			<p>WIRELESS SETUP</p> <p>Setup Select to setup basic wireless parameters.</p> <p>SSID</p>	

WLAN ACCESS RULES

Without wireless MAC access restriction, any wireless client can join (authenticate with) **21** work if they know the network name (also called the SSID) and perhaps a few other security parameters such as encryption keys.

When wireless MAC access is enabled, however, the access point or router performs an additional check on a different parameter. Obviously the more checks that are made, the greater the likelihood of preventing network break-ins.

To set up wireless MAC access rules, you as a WLAN administrator must configure a list of clients that will be allowed to join the network.

[Top](#)

MULTIPLE WLAN SSIDS

Multiple SSIDs **22**

The SSID is name of your WLAN. Do not use standard term, e.g. WLAN, as SSID.

The ASL-26555 supports Multiple SSIDs so you can operate several WLANs in parallel.

[Top](#)

WLAN PERFORMANCE

WLAN Performance **23**

Please note: The position of the ASL-26555 may influence the performance, specially the range of the radio signal.

Always change just one parameter and keep track of the effects.

Threshold for RTS

Default value: 2346

Generally there is no need to change this value. If the flow of traffic becomes inconsistent, change the value within the range between 256 and 2,3456.

Advice: If you have to change this value, do it in small steps and keep track of the effects.

SNMP

SNMP is short for Simple Network Management Protocol. This protocol provides functionality for controlling and monitoring networks. Trigger by defined events, e.g. errors, the protocol will inform the administrator in an appropriate way.

24

To use SNMP an additional software is necessary. Here you can set up the parameters for agent and traps only.

SNMP Agent

All devices monitored have to have an agent. These agents will send in regular intervals, on request or triggered by events data. The structure of this data is defined in MIBs.

Community

The SNMP community provides a simple access protection by creating a community named *public* with the "ReadOnly" right. A second community, named *admin* possesses the "ReadWrite" right, i.e. members of this community can edit the settings.

Via the community string a SNMP manager discloses his affiliation to a certain community. Unfortunately this string is transmitted as plaintext, making the security vulnerable.

Trap

A trap is send each time an event happens.

The message consists among other things of the common TrapID. 7 common TrapIDs are defined:

1. Cold boot
2. Warm boot
3. Link Down
4. Link Up
5. Authentication Error
6. EGP neighbour lost
7. internal information

[Top](#)

- En **Mantenimiento** hay seis ventanas:
1. La primera ventana es el índice de **Mantenimiento**
 2. La segunda ventana es la ventana **Administración**
 3. La tercera ventana es la ventana **Configuración del sistema**
 4. La cuarta ventana es la ventana **Actualización de firmware**
 5. La quinta ventana corresponde a la ventana **Prueba**
 6. La sexta es la ventana **Registro del sistema**

The screenshot displays the web interface for the ASL-26555 device. The top navigation bar includes 'ASL-26555', 'SETUP', 'ADVANCED', 'MAINTENANCE', 'STATUS', and 'HELP'. The 'MAINTENANCE' menu is expanded, showing a list of options: Administration, System Settings, Firmware Update, Test, and System Log. A red circle with the number '1' highlights the 'Administration' link. Below this, the 'ADMINISTRATION' section is visible, containing 'Administrator settings', 'User Settings', and various remote administration options (HTTP, TELNET, FTP, SAMBA, ICMP). A red circle with the number '2' highlights the 'Administrator settings' section. At the bottom of the page, the 'SYSTEM SETTINGS' section is visible, with a red circle and the number '3' highlighting the 'Save and Reboot the device' option. On the left side of the interface, there is a 'Menu' sidebar with options for 'Menu', 'Setup', 'Advanced', 'Maintenance', 'Status', and 'Logout'. A 'Zoom Level' dropdown is set to 'Middle', and a 'Reboot' button is present.

FIRMWARE UPDATE

To check for a new version for the *ASL -26555* click on the "Check" button. A new firmware version will have a high version number than the installed version. To update the firmware click on the "Update" button.



Warning! Never switch off the *ASL -26555* during a firmware update.

After the update check the settings on the "Internet" tab, page "DSL Access". Keep track of the behaviour of the *ASL -26555* while online.

[Top](#)

TEST

The Diagnostic Test page shows the test results for the connectivity of the physical layer and the data layer for both LAN and WAN sides.



[Top](#)

SYSTEM LOG

Remote Log Server collects the logs sent from our device with correct log level. Users can set a remote log server ip and the log level of our device. Then administrators are able to know the events that happen on our device.



There are five levels of message importance: System Activity, Debug Information, Attacks, Dropped Packets and Notice.

Select the levels that you want displayed in the log.

[Top](#)

BROADBAND

En **Estado** hay cinco ventanas:

1. La primera ventana es el índice de **Estado**
2. La segunda ventana es la **Información sobre el dispositivo**
3. La tercera ventana corresponde a la **Información de registro**
4. La cuarta ventana es la **Información USB**
5. La quinta ventana corresponde a las **Estadísticas**

The screenshot shows the web interface for the ASL-26555 device. At the top, it displays 'Product Page : ASL-26555' and 'Firmware Version : v2.0.0.33B_ES'. The main header features the 'ALPHA' logo and a navigation menu with tabs for 'ASL-26555 //', 'SETUP', 'ADVANCED', 'MAINTENANCE', 'STATUS', and 'HELP'. The left sidebar contains a 'Menu' with options: 'Setup', 'Advanced', 'Maintenance', 'Status', and 'Logout'. Below the menu, there is a 'Zoom Level' dropdown set to 'Middle' and a 'Reboot' button. The main content area is titled 'STATUS' and contains five sections, each with a red circular callout number:

- 1**: A list of links: [Device Info](#), [LOG Info](#), [USB Info](#), and [Statistics](#).
- 2**: The 'DEVICE INFO' section, which includes a description of the page and sub-sections for 'GENERAL', 'INTERNET STATUS', 'WIRELESS LAN', and 'LAN'.
- 3**: The 'LOG INFO' section, which describes the system log and includes a 'Refresh' button.
- 4**: The 'USB INFO' section, which displays USB-related information.
- 5**: The 'STATISTICS' section, which displays network statistics for LAN, WAN, Wireless, and ADSL.

Especificaciones técnicas

INTERFACES DE DISPOSITIVO

- Puerto ADSL RJ-11
- 4 puertos Ethernet RJ-45 10/100BASE-TX con auto MDI/MDIX
- 2 puertos USB (conector de tipo A)
- LAN inalámbrica 802.11n integrada
- Botón para restaurar a los valores de fábrica

LAN INALÁMBRICA

- Estándares 802.11b/g, 802.11n
- Velocidad inalámbrica: hasta 54Mbps (802.11g), 130Mbps (802.11n)
- Frecuencia: 2.4 GHz a 2.484G Hz
- Encriptación de datos a WEP 64/128 bits
- Seguridad WPA/WPA2 (acceso protegido Wi-Fi)
- SSID múltiples
- QoS inalámbrica 802.11e (WMM/WME)
- Control de acceso basado en direcciones MAC

ESTÁNDARES ADSL

- Estándares ADSL: multimodo, ANSI T1.413 versión 2, ITU G.992.1 (G.dmt) Anexo A, ITU G.992.2 (G.lite) Anexo A, ITU G.994.1 (G.hs)
- Estándares ADSL2: ITU G.992.3 (G.dmt.bis) Anexo A/L/M, ITU G.992.4 (G.lite.bis) Anexo A
- Estándares ADSL2+: ITU G.992.5 Anexo A/M

TASAS DE DATOS ADSL

- G.dmt: 8Mbps bajada, 832Kbps subida
- G.lite: 1.5Mbps bajada, 512Kbps subida
- ADSL2: 12Mbps bajada, 1Mbps subida
- ADSL2+: 24Mbps bajada, 1Mbps subida

PROTOCOLOS ATM Y PPP

- ATM Forum UNI3.1/4.0 PVC (hasta 16PVCs)
- Tipo de capa de adaptación ATM 5 (AAL5)
- QoS ATM (conformación del tráfico)

- Encapsulado Ethernet en modo bridge o enrutado
- Multiplexado basado en VC y LLC
- PPP sobre Ethernet (PPPoE)
- PPP sobre ATM (RFC 2364)
- ITU-T I.610 OAM F4/F5

FUNCIONES DEL ROUTER

- NAT (máximo 1024 sesiones NAT)
- Servidor/cliente/DHCP relay
- Enrutamiento estático, RIP v.1, v.2
- Universal Plug and Play (UPnP)
- Sistema de nombre de dominio dinámico (DDNS)
- Servidor virtual
- SNTP, proxy DNS y proxy IGMP

CORTAFUEGOS

- Cortafuegos NAT integrado
- Inspección de paquetes de datos (SPI)
- Prevención de ataques DoS
- Filtrado de paquetes (IP/ICMP/TCP/UDP)
- Sistema de detección de intrusos (IDS)
- DMZ

RED PRIVADA VIRTUAL (VPN)

Múltiples pasos PPTP/IPSec/L2TP

CONFIGURACIÓN/ADMINISTRACIÓN DE DISPOSITIVOS

- Asistente de instalación
- GUI web para la configuración y actualización del firmware
- Bloqueo de código para evitar las actualizaciones de firmware impropias
- Telnet con compatibilidad SSH
- Seguimiento Syslog

- SNMP v1, compatibilidad v2c con MIB-II integrado (RFC 1213)

CALIDAD DE SERVICIO

- Priorización/clasificación de tráfico LAN a WAN
- Priorización de tráfico 802.1p (0 a 7)
- Conformación del tráfico

SEGURIDAD

- Monitoreo IGMP con 32 grupos multidifusión
- Mapeo de puertos PVC/VLAN (modo bridge)
- Control parental (bloqueo URL, programación)

ALIMENTACIÓN

- A través de un transformador externo 12VAC 1.5A

LEDS DIAGNÓSTICOS

- Encendido
- LAN (1 a 4)
- WLAN
- DSL
- USB (1 a 2)

- Internet

DIMENSIONES

- 220 x 150 x 32 mm (8,66 x 5,90 x 1,26 pulgadas)

PESO

- 474 gramos (1.05 lb)

TEMPERATURA OPERATIVA

- 0° a 40° C (32° a 104° F)

TEMPERATURA DE ALMACENAMIENTO

- -20° a 70° C (-4° a 158° F)

HUMEDAD OPERATIVA

- 10% a 95% sin condensación

CERTIFICACIONES

- CE (EN55022/EN55024/EN300 328/ EN301 489)
- Certificación Wi-Fi
- Certificación K.21