MANUAL ZyXEL P320

Mayo 2006

INDICE

CAPÍTULO 1: CONOCIENDO SU P320W

Este capítulo describe las cualidades y aplicaciones de su Prestige

1.1 Introducción al Prestige P320W

Su Prestige es una router firewall inalámbrico para ser ubicado entre Internet y su LAN.

El dispositivo implementa funcionalidades NAT, firewall, servidor DHCP y muchas otras funciones avanzadas. El equipo dispone de un módulo mini-PCI integrado 802.11g para proporcionar un acceso inalámbrico en LAN.

El configurador web integrado es muy sencillo de manejar.

Nota : Utilice únicamente versiones de firmware específicas para su dispositivo.

1.2 Funcionalidades

Las siguientes secciones describen las funcionalidades soportadas por el P320W.

1.2.1 Funcionalidades Físicas

Interfaces Fast Ethernet 10/100 Mbps con Auto-negociación

Esta funcionalidad de auto-negociación permite al dispositivo detectar la velocidad de las transmisiones y ajustarse de forma automática sin necesidad de intervención manual. Este permite disfrutar tasas de transferencia de10Mbps ó 100Mbps así como del modo half-dúplex o full-duplex en función de la red Ethernet.

Interfaces Fast Ethernet 10/100 con Auto-crossover

Estas interfaces se ajustan también de forma automática y son capaces de funcionar correctamente tanto si se utiliza un cable recto o uno cruzado.

Switch integrado de 4 puertos

La combinación de router y switch hacen del P320W una solución efectiva para ser ubicada en una pequeña red doméstica. Es posible añadir hasta cuatro ordenador al equipo sin necesidad de ningún hub externo. Puede seguir añadiendo más dispositivos en la LAN mediante la utilización de un hub/switch adicional.

Botón de reset

El botón de reset del router se encuentra ubicado en el panel posterior. Utilice este botón para restaurar la contraseña por defecto 1234; la dirección IP a 192.168.1.1, la máscara de subred a 255.255.255.0 y el servidor DHCP habilitado con un pool de 32 direcciones IP comenzando por la 192.168.1.33.

1.2.2 Funcionalidades No-Físicas

Firewall

El equipo dispone de un firewall SPI (Stateful Packet Inspection) con protección DoS (Denial of Service). Por defecto, cuando el firewall está activado, todo el tráfico entrante desde la WAN hacia la LAN es bloqueado a menos que haya sido iniciado previamente desde la LAN. El router suporta inspección TCP/UDP, detección y prevención DoS, alertas en tiempo real, informes y logs.

Filtrado de paquetes

El mecanismo del filtrado de paquetes bloquea el que todo el tráfico no deseado pueda entrar/salir de la red.

Hora y Fecha

El equipo permite obtener la fecha y hora actual de un servidor externo. También es posible configurar estos parámetros de forma manual.

Universal Plug and Play (UPnP)

Utilizando el protocolo TCP/IP, nuestro dispositivo junto con cualquier otro dispositivo con el UPnP habilitado pueden establecer una red de forma dinámica, obtener una dirección IP y proporcionar sus capacidades a otros dispositivos de la red.

PPPoE

La encapsulación PPPoE facilita la interacción de un host con Internet para lograr el establecimiento de un acceso de alta velocidad mediante la utilización de un interfaz de usuario similar a la de una conexión telefónica a red.

Encapsulación PPTP

La encapsulación PPTP es un protocolo de red que posibilita transferencias de datos seguras desde un cliente remoto a un servidor privado, mediante la creación de una VPN utilizando la red TCP/IP.

Este dispositivo soporta una conexión con un servidor PPTP de forma simultánea.

Soporte DNS Dinámico

Mediante esta funcionalidad de DNS Dinámico, es posible disponer de un nombre de host estático asociado a una dirección IP dinámica, permitiendo a un determinado host el ser accesible de forma más sencilla desde cualquier punto de Internet. Es necesario registrarse, para usar este servicio, con el proveedor Dynamic DNS.

Multicast IP

Esta función permite distribuir un paquete IP a un grupo específico de host utilizando una dirección IP multicast. IGMP es el protocolo utilizado para soportar los grupos multicast. El gateway soporta tanto la versión 1 como la 2.

SNMP

SNMP es un protocolo utilizado para intercambiar información de gestión entre los dispositivos de red. El router soporta la funcionalidad de agente SNMP, lo que permite a una estación gestora el controlar y monitorizar a este dispositivo a través de la red. El P320W soporta SNMP versión 1 (SNMPv1) y la versión 2 (SNMPv2).

Network Address Translation (NAT)

La funcionalidad NAT permite la traslación de una dirección Internet utilizada dentro de una red (por ejemplo, una dirección IP privada utilizada en una red local) a una dirección IP diferente conocida dentro de otra red (por ejemplo, una dirección IP pública utilizada en Internet).

Redirección de Tráfico

La funcionalidad de redirección de tráfico permite redirigir el tráfico WAN hacia un gateway de backup situado en la LAN cuando el router no puede conectarse con Internet, lo que proporciona un backup auxiliar cuando la conexión WAN habitual falla.

Redirección de puertos

Utilice esta funcionalidad para permitir el acceso de determinadas peticiones de servicio hacia un servidor colocado en la red local. Será necesario introducir el número de puerto individual o rango de puertos que serán redirigidos así como la dirección IP que vaya a hacer de servidor en la red interna.

DHCP (Dynamic Host Configuration Protocol)

El protocolo DHCP permite que ordenadores de cliente obtengan la configuración TCP/IP desde un servidor DHCP centralizado. El router incorpora un servidor DHCP, habilitado por defecto, lo que significa que podrá asignar direcciones IP, la dirección IP

del gateway así como de los servidores DNS a todos los equipos que se conecten en la red interna y tengan configurado un cliente DHCP.

Gestión de red completa

El configurador web integrado permite el acceso sencillo a la configuración y visualización de los parámetros del router.

Registro de logs

Se incorpora un mecanismo interno capaz de registrar diferentes eventos así como de capturar trazas de paquetes.

Servidor FTP y TFTP integrados

El gateway incorpora servidor FTP y TFTP habilitados que permiten realizar las actualizaciones de firmware de forma rápida y sencilla, así como backups y restauraciones de la configuración.

1.2.3 Funcionalidades Wireless

Wireless LAN

El router soporta el estándar IEEE 802.11g, totalmente compatible con el estándar 802.11b, lo que significa que se podrán tener tanto clientes 802.11b como 802.11g en la misma red inalámbrica.

Nota : El router puede ser interferido por otros dispositivos trabajando en el rango de los 2.4GHz tales como hornos microondas, teléfonos inalámbricos, dispositivos bluetooth así como otros dispositivos inalámbricos.

Wi-Fi Protected Access

Wi-Fi Protected Access (WPA) es un subconjunto de las especificaciones de seguridad definidas en el estándar IEEE 802.11i. Las principales diferencias entre WPA y WEP son la autenticación de usuario y la mejora en la encriptación de datos.

Antena

El router está equipado con una antena fija de 2dBi para proporcionar una señal radio clara entre las estaciones inalámbricas y los puntos de acceso.

Filtrado MAC

El dispositivo puede comparar la dirección MAC de las direcciones inalámbricas con una lista de direcciones MAC a las que se permite o no el acceso.

Encriptación WEP

WEP (Wired Equivalent Privacy) encripta las tramas de datos antes de ser transmitidas por la red inalámbrica para ayudar a mantener la privacidad de las comunicaciones de red.

OTIST (One Touch Intelligent Security Technology)

OTIST permite al router asignar su SSID y parámetros de seguridad (WEP ó WPA-PSK) a los adaptadores inalámbricos ZyXEL que también soporten esta funcionalidad.

Lista de asociación

Con la lista de asociación, es posible visualizar la lista de estaciones inalámbricas que se encuentran actualmente asociadas a nuestro gateway.

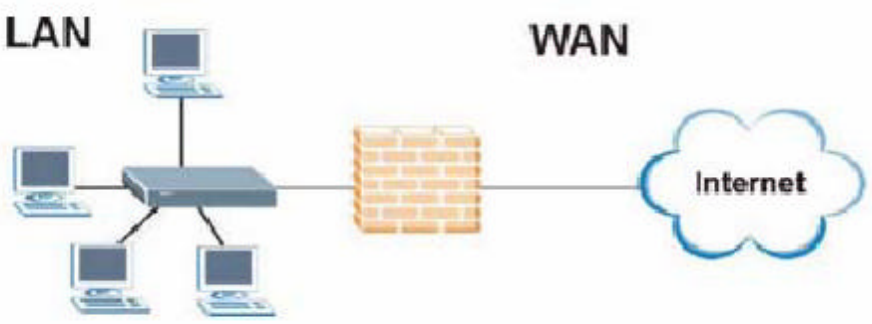
1.3 Aplicaciones del P320W

Aquí se muestran algunos ejemplos de lo que nuestro dispositivo puede ofrecer.

1.3.1 Acceso a Internet seguro mediante módem cable o DSL

Es posible conectar un cablemódem, o módem DSL a este dispositivo para disfrutar de un acceso a Internet tanto a usuarios Ethernet como inalámbricos. El P320W garantiza no sólo un acceso a Internet de alta velocidad, sino que también proporcionará una protección a la red interna así como gestión del tráfico.

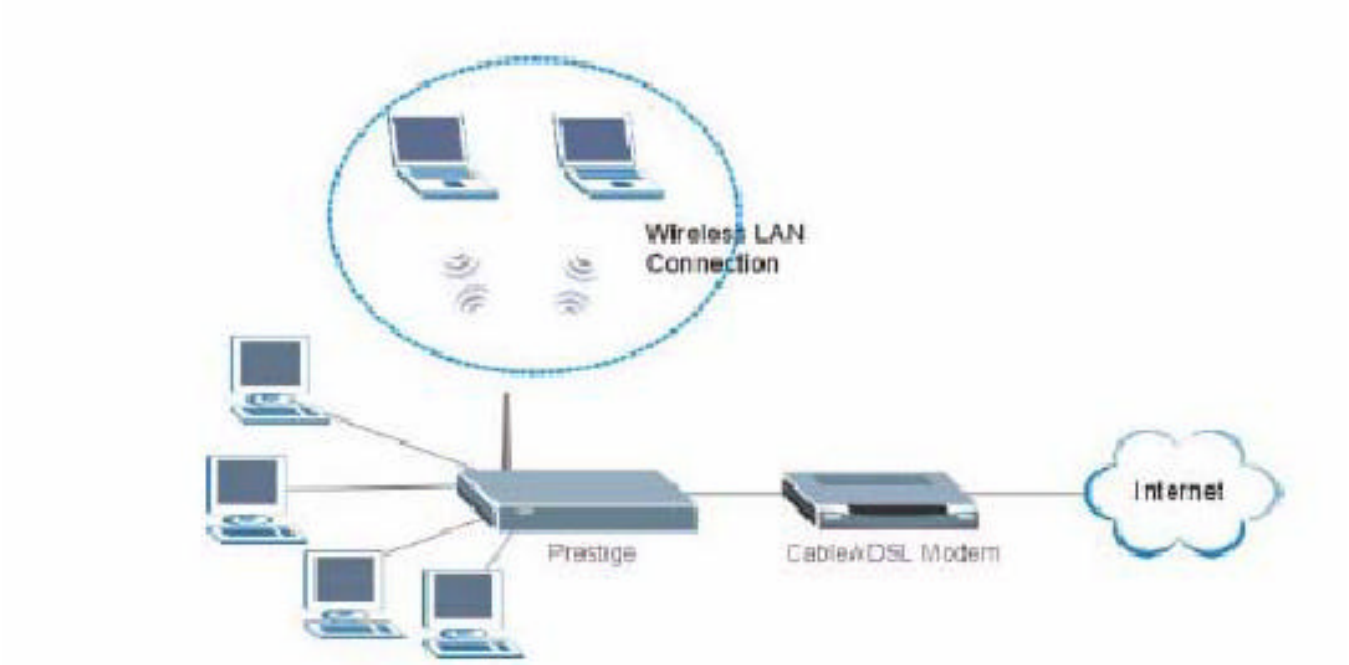
Figura 1 Acceso a Internet



1.3.2 Aplicación de LAN Inalámbrica

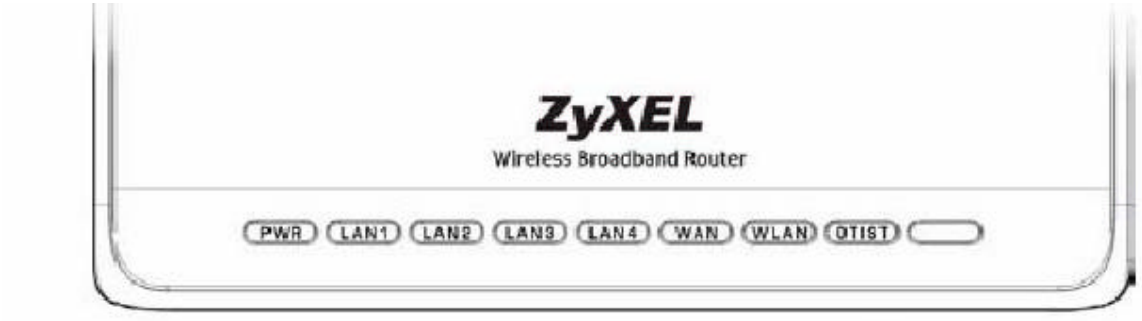
Añada un acceso inalámbrico a su LAN existente, de manera que las estaciones wireless puedan desplazarse libremente dentro de cualquier zona del área de cobertura y seguir disfrutando de los mismos recursos de red la red cableada.

Figura 2 Ejemplo de Aplicación de Acceso a Internet



1.3.3 LEDs del Panel Frontal

Figura 3 Panel Frontal



La siguiente tabla describe estos LEDs.

Tabla 1 LEDs del Panel Frontal

LED	COLOR	ESTADO	DESCRIPCIÓN
PWR	Verde	On	El router está siendo alimentado y funcionando correctamente
		Parpadeando	El router está realizando un análisis interno
	Rojo	On	La potencia que está recibiendo el router es demasiado baja
	Ninguno	Apagado	El router no está siendo alimentado
LAN 1-4	Verde	On	El router tiene establecida una conexión Ethernet 10Mb
		Parpadeando	El router está enviando/recibiendo datos
	Naranja	On	El router tiene establecida una conexión Ethernet 100Mb
		Parapadeando	El router están enviando/recibiendo datos
	Ninguno	Apagado	La LAN no está conectada
WAN	Verde	On	El router tiene establecida una conexión Ethernet 10Mb
		Parpadeando	El router está enviando/recibiendo datos
	Naranja	On	El router tiene establecida una conexión Ethernet 100Mb
		Parapadeando	El router están enviando/recibiendo datos
	Ninguno	Apagado	La WAN no está conectada
WLAN	Verde	On	El router está preparado, pero no está enviando/recibiendo datos a través del interfaz inalámbrico
		Parpadeando	El router está enviando/recibiendo datos a través del interfaz inalámbrico
	Ninguno	Apagado	El interfaz inalámbrico no está activado
OTIST	Verde	Parpadeando	OTIST en progreso
		On	OTIST está activado y los parámetros de seguridad inalámbricos han sido transferidos a los clientes wireless. El LED se mantiene sin utilidad a no ser que se modifiquen los parámetros WLAN.
	Ninguno	Apagado	OTIST no está activado o los parámetros WLAN han sido configurados manualmente tras una operación OTIST.

CAPÍTULO 2: INTRODUCCIÓN AL CONFIGURADOR WEB

Este capítulo describe como acceder al router a través del configurador Web proporcionando una descripción de sus pantallas.

2.1 Descripción Configurador Web

El configurador Web presenta una interfaz de gestión basada en HTML que permite una configuración y gestión sencilla del equipo a través de un navegador de Internet. Utilizar versiones de Internet Explorer 6.0 o posteriores o Netscape Navigator 7.0 o posteriores. La resolución recomendada de pantalla es de 1024x768 pixels.

Para utilizar el configurador Web será necesario:

• Navegador Web con ventanas pop-up habilitadas en su equipo. Los pop-ups web están habilitadas por defecto enWindows XP SP 2.

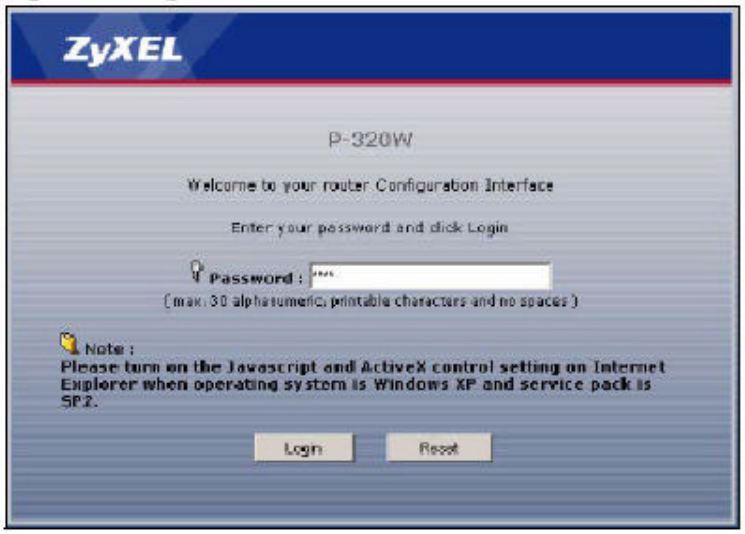
• JavaScripts (habilitados por defecto)

• Permisos Java (habilitados por defecto).

2.2 Accediendo al Configurador Web

1. Asegure que el hardware de su router se encuentre correctamente conectado y prepare su ordenador para conectarse al su P320W.
2. Lance su navegador web.
3. Introduzca “192.168.1.1” como dirección URL.
4. Introduzca “1234” (defecto) como password y pulse sobre **Login (Acceder)**.

Figura 4 Login

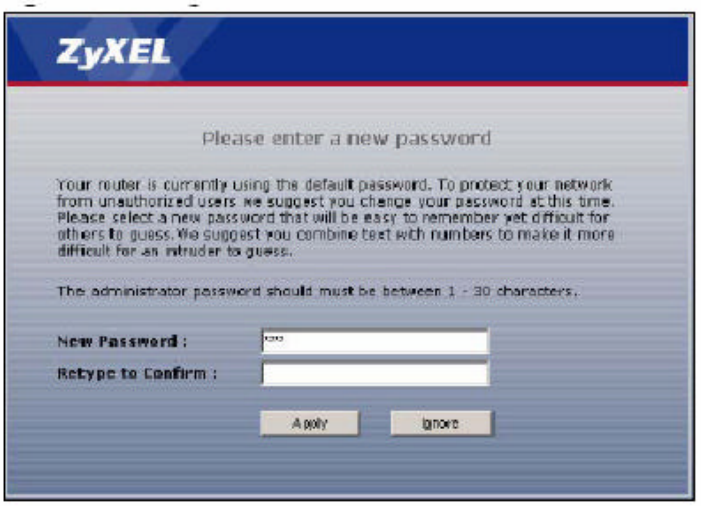


5. Seleccione su idioma. Pulse sobre **Apply (Aplicar)**.

Figura 5 Selección del Idioma

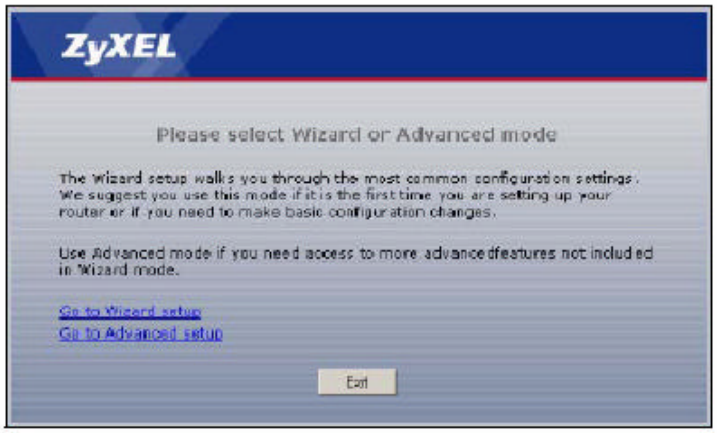
6. Deberá ver la siguiente ventana solicitando el cambio de la contraseña de acceso (muy recomendado) como se muestra a continuación. Introduzca la nueva contraseña (y repítala para su confirmación) y pulse **Apply (Aplicar)** o pulse sobre **Ignore (Ignorar)** para no realizar ningún cambio.

Figura 6 Pantalla Cambio de Contraseña



7. Pulse sobre **Go to Wizard Setup (Vaya a configuración con asistente)** para realizar una configuración inicial utilizando este asistente, pulse sobre **Go to Advanced Setup (Vaya a configuración avanzada)** para configurar las funcionalidades avanzadas, o pulse **Exit (Salir)** para salir del configurador Web.

Figura 7 Selección del Modo



Nota: La sesión de gestión se desconectará automáticamente cuando el periodo de tiempo configurado en el campo **Administrator Inactivity Timer (Temporizador de inactividad del administrador)** expire (por defecto, 5 minutos).

2.3 Resetear el P320W

Si olvidase la contraseña o no pudiese acceder al configurador Web, será necesario utilizar el botón **RESET** en la parte posterior del router para cargar los parámetros de

configuración por defecto. Este significa que se perderá toda la configuración previamente realizada y la contraseña volverá a ser “1234”.

2.3.1 Procedimiento de Uso del Botón de Reset

1. Asegure que el LED **PWR** está fijo (sin parpadear).
2. Presione el botón de **RESET** durante unos 10 segundos o hasta que el LED **PWR** comience a parpadear y a continuación suéltelo. Cuando el LED **PWR** comience a parpadear, los parámetros por defecto han sido restaurados y el router se reinicia.

2.4 Navegación por el Configurador Web

A continuación se resume como navegar por el configurador web desde la pantalla **Status (Estado)**.

Figura 8 Pantalla Estado del Configurador Web

La siguiente tabla describe los iconos mostrados en la pantalla de **Estado**.

Tabla 2 Iconos de la Ventana Estado

ICONO	DESCRIPCIÓN
	Seleccione el idioma de la lista desplegable para hacer que el router muestre el configurador web en el idioma que se seleccione.
	Pulse este icono para abrir la página de ayuda relativa a la pantalla de configuración que se está utilizando
	Pulse sobre este icono para abrir el asistente de configuración. El router dispone de un asistente de conexión y un asistente de gestión de ancho de banda.
	Pulse sobre este ico para visualizar los derechos de copia y un enlace con información relativa al producto.
	Pulse sobre este icono en cualquier momento para salir del configurador web.
	Seleccione el número de segundos o **None (Ninguno)** de la lista desplegable para refrescar todas las estadísticas automáticamente al cabo del intervalo de tiempo configurado o no refrescar dicha información
	Pulse sobre este botón para refrescar las estadísticas de la pantalla de estado.

Tabla 3 Pantalla de Estado del Configurador Web

ETIQUETA	DESCRIPCIÓN
Información del Dispositivo	
Nombre del Sistema	Este es el Nombre del Sistema que se introduce en la pantalla Administración, Sistema, General. Únicamente con propósitos informativos.
Versión de Firmware	Aquí se muestra la versión de firmware y la fecha en la que fue creada.
Información WAN	
- Tipo WAN	Este campo muestra el modo de encapsulación
- Dirección IP	Este campo muestra la dirección IP del puerto WAN
- Máscara de Subred	Este campo muestra la máscara de subred del puerto WAN
- Puerta de enlace	Este campo muestra la dirección IP de la puerta de enlace
- DNS	Este campo muestra la(s) dirección(es) de los servidores DNS
Información LAN	
- Dirección IP	Este campo muestra la dirección IP del puerto LAN
- Máscara de subred	Este campo muestra la máscara de subred del puerto LAN
- DHCP	Este campo muestra si el router actúa o no como servidor DHCP.
Información WLAN	
- Nombre (SSID)	Este campo muestra el nombre descriptivo utilizado para identificar el router en la red inalámbrica
- Canal	Este campo muestra el número de canal utilizado por el router en la red inalámbrica
- Modo de Seguridad	Este campo muestra el nivel de seguridad que el

	router está utilizando
Estado del Sistema	
Tiempo del Sistema	Este campo muestra el tiempo que el sistema lleva encendido
Fecha/Hora Actual	Este campo muestra la fecha y hora actuales junto con la diferencia horaria con la zona GMT. Este valor se encontrará ajustado al horario de verano si el equipo se ha configurado para ello.
Resumen	
Tabla DHCP	Utilice esta pantalla para visualizar la información sobre clientes DHCP
Lista de asociaciones	Utilice esta pantalla para visualizar las estaciones que se encuentran actualmente conectadas al P320W
Estadísticas	Utilice esta pantalla para visualizar el estado de los puertos y las estadísticas de paquetes

2.4.1 Panel de Navegación

Tras introducir la contraseña de acceso, utilice los submenús en el panel de navegación para configurar las distintas funcionalidades del gateway.

La siguiente tabla describe estos submenús.

Tabla 4 Resumen de pantallas

ENLACE	PESTAÑA	FUNCIÓN
Estado (Status)		Esta pantalla muestra información general del dispositivo y del estado del sistema. Utilice esta pantalla para acceder al asistente de configuración y a las tablas resumen de estadísticas.
Red		
LAN Inalámbrica	General	Utilice esta pantalla para configurar la LAN inalámbrica
	OTIST	Esta pantalla permite asignar a los clientes inalámbricos del router los parámetros de seguridad del P320W
	Filtrado MAC	Utilice el filtrado MAC para configurar el router y bloquear el acceso a dispositivos o permitir a los dispositivos el acceso al mismo
	Avanzada	Esta pantalla permite configurar otras propiedades avanzadas WLAN
WAN	Conexión a Internet	Este pantalla permite configurar parámetros del ISP, asignación de dirección IP de WAN y dirección MAC de WAN.
	Avanzada	Utilice esta pantalla para configurar los servidores DNS
	Redirección de Tráfico	Utilice esta pantalla para configurar las propiedades y los parámetros de la redirección de tráfico.
LAN	IP	Utilice esta pantalla para configurar los parámetros de LAN.
Servidor DHCP	General	Utilice esta pantalla para habilitar el servidor DHCP del router y los servidores DNS a asignar por el servidor DHCP.
	DHCP Estático	Utilice esta pantalla para asignar direcciones IP en la LAN a ordenadores específicos basados en sus direcciones MAC
	Lista de	Utilice esta pantalla para visualizar la información sobre los clientes

	Clientes	DHCP siempre con la asignación entre dirección IP y dirección MAC
NAT	General	Utilice esta pantalla para habilitar el NAT
	Reenvío de puertos	Utilice esta pantalla para configurar servidores tras el router
	Lanzamiento de puertos	Utilice esta pantalla para modificar los parámetros de puertos dinámicos en el router
Seguridad		
Cortafuegos	General	Utilice esta pantalla para activar/desactivar el firewall
	Servicios	Esta pantalla muestra las reglas del firewall, y permite editar/añadir una regla en el firewall
Administración		
Rutas estáticas	Reglas de rutas estáticas	Utilice esta pantalla para configurar rutas estáticas
MGMT a distancia (Gestión remota)	WWW	Utilice esta pantalla para configurar a través de que interfaz (o interfaces) y desde que dirección (o direcciones) IP se podrá gestionar el dispositivo mediante HTTP.
	SNMP	Utilice esta pantalla para configurar los parámetros SNMP de su router.
	Seguridad	Utilice esta pantalla para modificar los parámetros anti-probing de su equipo.
UPnP	General	Utilice esta pantalla para habilitar UPnP
Mantenimiento		
Sistema	General	Esta pantalla contiene información administrativa.
	DNS Dinámico	Utilice esta pantalla para configurar el DNS Dinámico
	Ajuste de la hora	Utilice esta pantalla para modificar los parámetros de fecha y hora de su gateway
Registros	Ver registro	Utilice esta pantalla para visualizar los logs de las categorías seleccionadas.
	Configuración del registro	Utilice esta pantalla para modificar los parámetros de logs de su router.
Herramientas	Firmware	Utilice esta pantalla para actualizar el firmware de su equipo.
	Configuración	Utilice esta pantalla para realizar un backup o restaurar la configuración o restaurar los parámetros por defecto en su dispositivo
	Reiniciar	Esta pantalla permite reiniciar el router sin necesidad de apagar el equipo.

2.4.2 Resumen: Tabla DHCP

El protocolo DHCP permite a clientes individuales el obtener la configuración TCP/IP desde un servidor DHCP. El P320W puede ser configurado con servidor DHCP. Si el servicio DHCP se deshabilita, será necesario disponer de otro servidor DHCP en la LAN, o configurar de forma manual los parámetros TCP/IP de cada ordenador.

Pulse sobre **Tabla DHCP (Detalles)** en la pantalla **Estado (Status)**. La información de sólo-lectura que aparece aquí está referida al estado del DHCP. La tabla DHCP muestra la información (incluyendo Dirección IP, Nombre de Host y Dirección MAC) de todos los clientes haciendo uso del servidor DHCP del gateway.

Figura 9 Resumen: Tabla DHCP

La siguiente tabla describe los campos de esta pantalla.

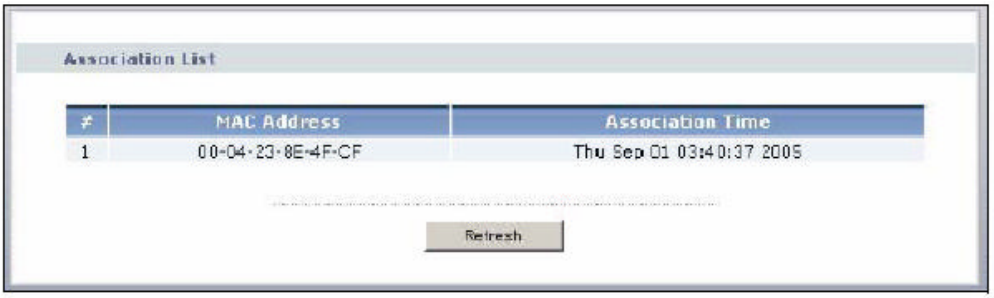
Tabla 5 Resumen: Tabla DHCP

ETIQUETA	DESCRIPCIÓN
#	Este campo muestra el índice que corresponde con el ordenador de cliente
Dirección IP	Este campo muestra la dirección IP relativa al campo # mostrado anteriormente
Nombre del Host	Este campo muestra el nombre del ordenador
Dirección MAC	Este campo muestra la dirección MAC del ordenador con el nombre de host anterior. Cada dispositivo Ethernet dispone de una dirección MAC única. La dirección MAC es asignada durante el proceso de fabricación y consiste en seis pares de caracteres hexadecimales, por ejemplo, 00:A0:C5:00:00:02
Actualizar	Pulse sobre **Actualizar** para devolver los parámetros originales de pantalla.

2.4.3 Resumen: Lista de Asociaciones

Pulse sobre **Lista de Asociaciones (Detalles)** en la pantalla de **Estado (Status),** visualizando las estaciones inalámbricas actualmente asociadas al router.

Figura 10 Resumen: Lista de Asociaciones



La siguiente tabla describe las etiquetas de esta pantalla.

Tabla 6 Resumen: Lista de asociaciones inalámbricas

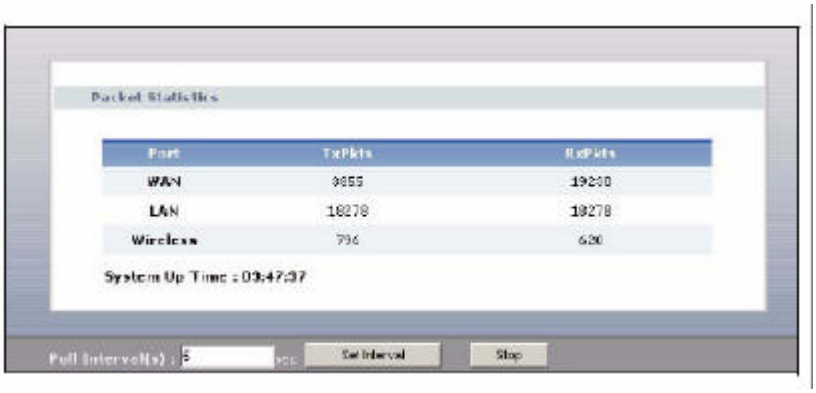
ETIQUETA	DESCRIPCIÓN
#	Este campo muestra el índice de la estación inalámbrica asociada
Dirección MAC	Este campo muestra la dirección MAC de la esación inalámbrica
Tiempo de asociación	Este campo muestra el tiempo en que el cliente se asoció por primera vez al router

Refrescar	Pulse sobre **Refrescar** para volver a visualizar los datos de la pantalla.

2.4.4 Resumen: Estadísticas de Paquetes

Pulse en el enlace **Estadísticas (Detalles)** en la pantalla de **Estado (Status)**. La información de sólo-lectura mostrada en esta pantalla incluye las estadísticas específicas de cada paquete. También se muestra información sobre el tiempo que el sistema lleva levantado y el intervalo de refresco. El campo de **Intervalo de Actualización** es configurable.

Figura 11 Resumen: Estadísticas de Paquetes



La siguiente tabla describe las etiquetas de esta pantalla.

ETIQUETA	DESCRIPCIÓN
Puerto	Este campo indicará el puerto LAN, WAN o WLAN.
TxPkts	Este campo muestra el número de paquetes transmitidos por el puerto.
RxPkts	Este campo muestra el número de paquetes recibidos por el puerto.
Tiempo del sistema	Este campo muestra el tiempo total que el router lleva encendido
Intervalo de sondeo	Este campo permite introducir el intervalo de tiempo en que las estadísticas de esta pantalla van a ser actualizadas.
Ajustar el intervalo	Pulse este botón para aplicar el nuevo intervalo de sondeo introducido en el campo anterior.
Detener	Pulse **Detener** para detener la actualización de estadísticas.

CAPÍTULO 3: ASISTENTE DE CONFIGURACIÓN

Este capítulo proporciona información sobre las pantallas del asistente de conexión del configurador Web.

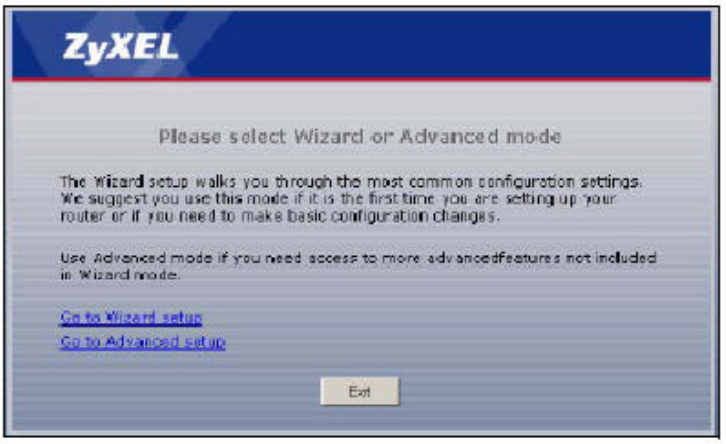
3.1 Asistente de Configuración

El asistente de configuración Web permite configurar los parámetros del dispositivo para el acceso a Internet.

1. Tras acceder al configurador Web del gateway, pulse sobre **Go to Wizard setup (Vaya al configuración con asistente)**.

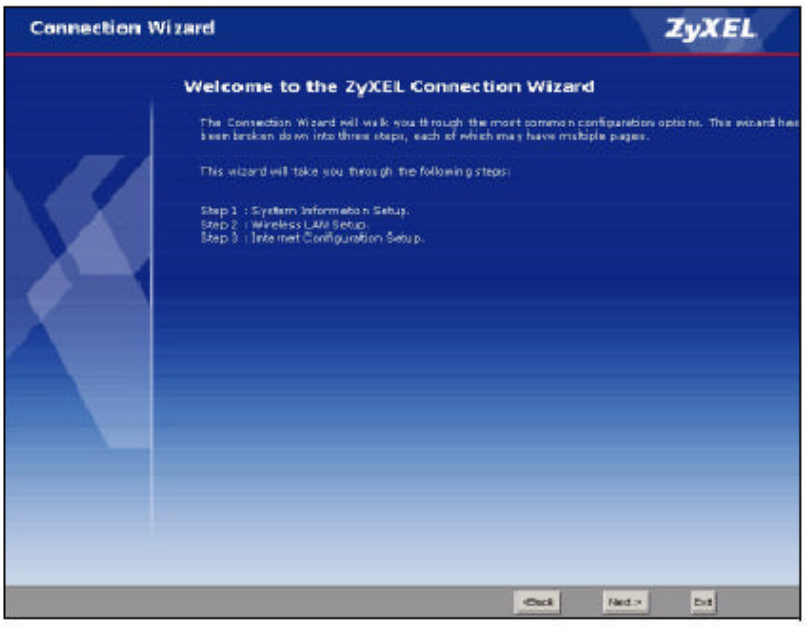
También podrá pulsar sobre el enlace **Go to Advanced setup (Vaya a configuración avanzada)** para saltar este asistente y proceder con la configuración de funciones avanzadas.

Figura 12 Selección del modo



2. Revise la información que aparece en la pantalla y pulse **Siguiente.**

Figura 13 Bienvenido al Asistente de Conexión



3.2 Asistente de conexión: PASO 1: Información del Sistema

La parte de **Información del Sistema** contiene información administrativa y relativa al sistema.

3.2.1 Nombre del Sistema

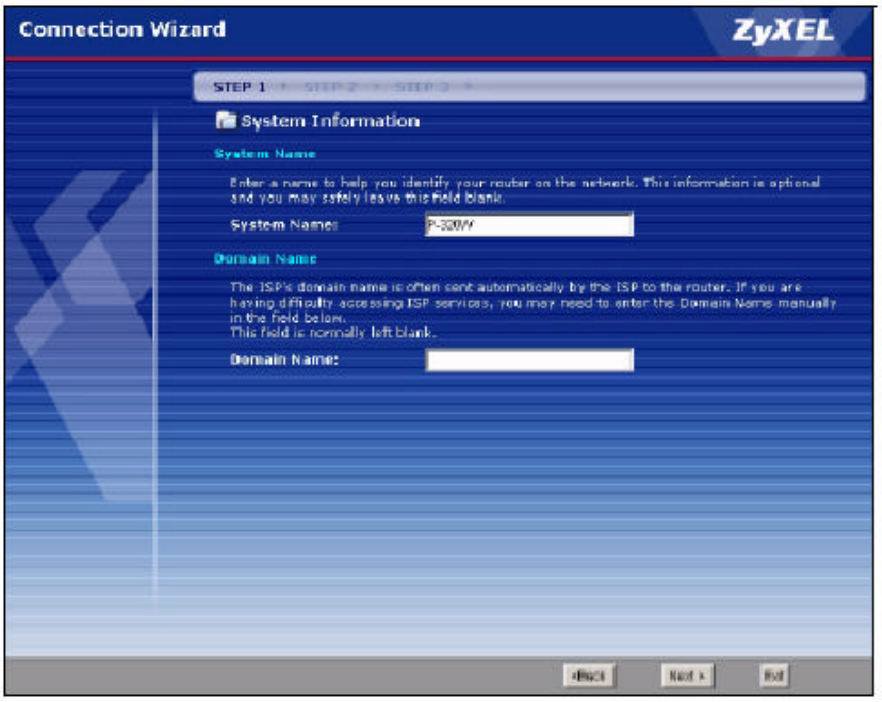
El campo **Nombre del Sistema** se utiliza meramente como un campo de carácter identificativo.

3.2.2 Nombre de Dominio

La entrada del campo Nombre de Dominio es el valor que se envía a los clientes DHCP ubicados en la LAN. Si este campo se deja en blanco, el nombre de dominio que se utilizará será el que se reciba por DHCP del ISP (en caso de utilizarse).

Pulse **Siguiente** para configurar el acceso a Internet en el gateway.

Figura 14 Asistente de conexión: PASO 1: Información del Sistema



La siguiente tabla describe las etiquetas en esta pantalla.

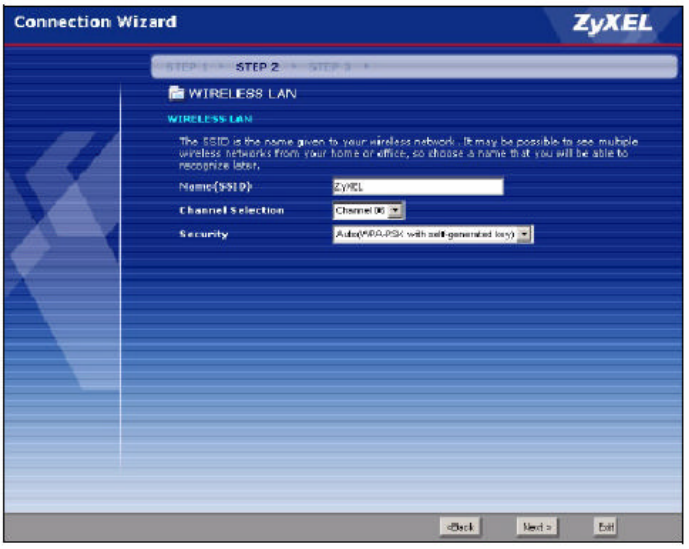
Tabla 8 Asistente de conexión: PASO 1: Información del sistema

ETIQUETA	DESCRIPCIÓN
Nombre del sistema	El nombre del sistema es un nombre único para identificar al gateway dentro de una red ethernet. Este campo puede contener hasta 30 caracteres.
Nombre de dominio	Introduzca el nombre de dominio si dispone de alguno. En caso de no disponer del mismo, deje este campo en blanco.
Atrás	Pulse **Atrás** para volver a la pantalla anterior.
Siguiente	Pulse **Siguiente** para pasar a la siguiente pantalla.
Salir	Pulse **Salir** para cerrar el asistente de configuración sin guardar los cambios realizados.

3.3 Asistente de conexión : PASO 2: LAN Inalámbrica

Configure su LAN Inalámbrica utilizando la siguiente pantalla.

Figura 15 Asistente de conexión: PASO 2 : LAN Inalámbrica



La siguiente tabla describe las etiquetas de esta pantalla.

Tabla 9 Asistente de conexión: PASO 2: LAN Inalámbrica

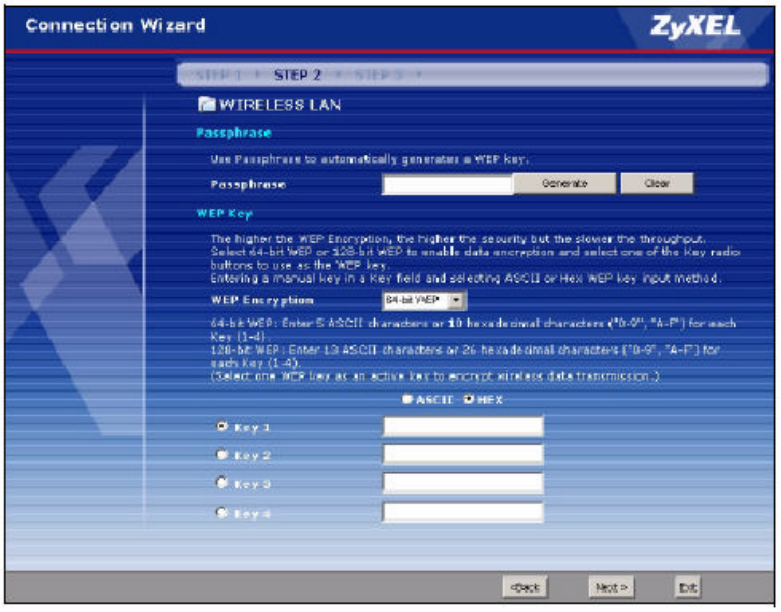
ETIQUETA	DESCRIPCIÓN
Nombre (SSID)	Introduzca un nombre descriptivo (hasta 32 caracteres) para la LAN inalámbrica. Si modifica este campo en su gateway, asegúrese que todas las estaciones inalámbricas utilizan el mismo SSID para seguir manteniendo el acceso a la red.
Selección de canal	El rango de frecuencias utilizados por los estándares IEEE 802.11b/g es denominado canal. Seleccione un canal para su dispositivo que no esté siendo utilizado por algo otro dispositivo inalámbrico cercano.
Seguridad	Selecciona un nivel de seguridad de la lista desplegable. Seleccione la opción **Auto (WPA-PSK con clave autogenerada)** para utilizar el modo de seguridad WPA-PSK con una clave por defecto predefinida y únicamente si sus clientes soportan WPA-PSK. Si escoge esta opción, vaya directamente a la sección 3.3.3. Seleccione **Ninguna** para no configurar ningún tipo de seguridad en su LAN inalámbrica. Si no habilita ninguna seguridad, su red será accesible por cualquier dispositivo inalámbrico dentro de la zona de cobertura. Si se escoge esta opción, vaya directamente a la sección 3.3.3. Seleccione la opción **Básica (WEP)** si desea configurar los parámetros de encriptación WEP. Si selecciona esta opción, vaya directamente a la sección 3.3.1. Seleccione la opción de seguridad **Extendida (WPA-PSK con clave personalizada)** para configurar una clave determinada. Escoja esta opción si sus clientes inalámbricos soportan WPA-PSK. Si esta es su elección, pase a
	la sección 3.3.2.
Atrás	Pulse **Atrás** para volver a la pantalla anterior.
Siguiente	Pulse **Siguiente** para pasar a la siguiente pantalla.
Salir	Pulse **Salir** para salir del asistente sin guardar ningún cambio.

Nota: Las estaciones inalámbricas y el P320W deben utilizar el mismo SSID, el mismo canal y el mismo tipo de encriptación para una comunicación inalámbrica correcta.

3.3.1 Seguridad Básica (WEP)

Seleccione Básica (WEP) para configurar los parámetros de encriptación WEP.

Figura 16 Configuración Básica (WEP)



La siguiente tabla describe las etiquetas de esta pantalla.

Tabla 10 Seguridad Básica (WEP)

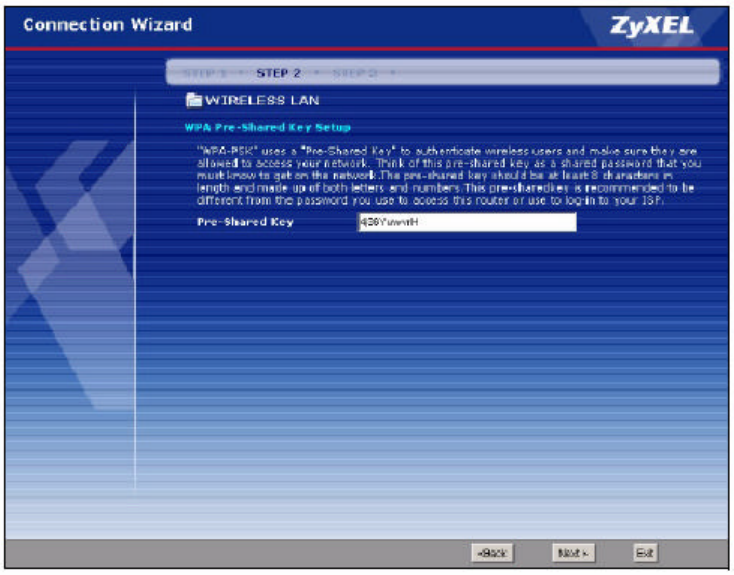
ETIQUETA	DESCRIPCIÓN
Frase secreta	Introduzca una frase (de hasta 32 caracteres) y pulse sobre el botón **Generar**. El router automáticamente generará las cuatro claves WEP.
Generar	Tras introducir una frase, pulse **Generar** para que el router genere automáticamente las claves WEP.
Borrar	Pulse **Borrar** para descartar la frase configurada en el campo Frase secreta.
Cifrado WEP	Seleccione 64-bit WEP ó 128-bit WEP
ASCII	Seleccione esta opción para introducir valores ASCII como claves WEP.
HEX	Seleccione esta opción para introducir caracteres hexadecimanes como claves WEP. El valor "0x" se introduce automáticamente.
Clave 1 a Clave 4	Las claves WEP son utilizadas para encriptar los datos. Tanto el P320W como las estaciones inalámbricas deben utilizar la misma clave WEP para la transmisión de datos.

	Si selecciona el modo 64-bit WEP, entonces introduzca bien 5 caracteres ASCII ó 10 caracteres hexadecimales ("0-9", "A-F") Si selecciona el modo 128-bit WEP, entonces introduzca bien 13 caracteres ASCII ó 26 caracteres hexadecimales ("0-9","A-F"). Deberá configurar al menos una clave, únicamente una clave podrá estar activa de forma simultánea. La clave por defecto es la clave 1.
Atrás	Pulse **Atrás** para mostrar la pantalla anterior.
Siguiente	Pulse **Siguiente** para pasar a la siguiente pantalla.
Salir	Pulse **Salir** para salir del asistente sin guardar los cambios.

3.3.2 Seguridad Extendida (WPA-PSK)

Seleccione la seguridad Extendida (WPA-PSK) en la pantalla de LAN inalámbrica para configurar una clave determinada.

Figura 17 Seguridad Extendida (WPA-PSK)



La siguiente tabla describe las etiquetas de esta pantalla.

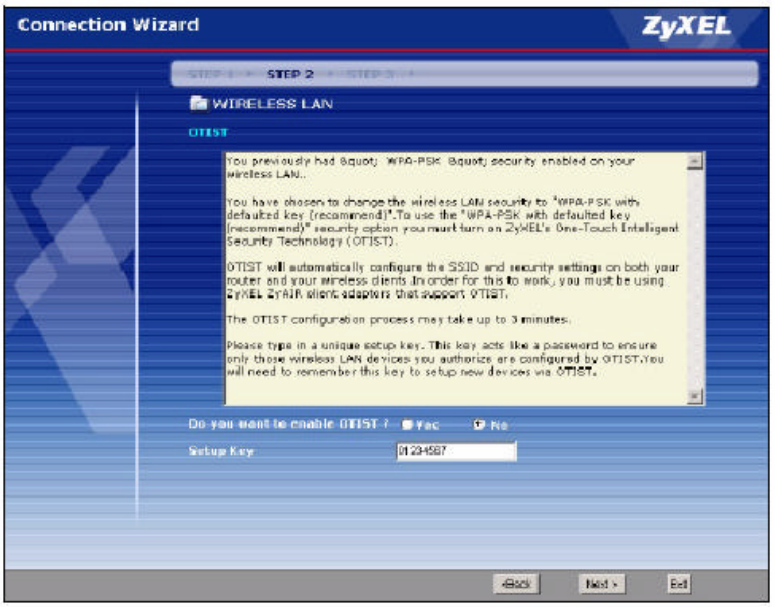
Tabla 11 Seguridad Extendida (WPA-PSK)

ETIQUETA	DESCRIPCIÓN
Clave pre-establecida	Introduzca una clave entre 8 y 63 caracteres con diferenciación entre mayúsculas y minúsculas.
Atrás	Pulse **Atrás** para mostar la pantalla anterior.
Siguiente	Pulse **Siguiente** para mostrar la siguiente pantalla.
Salir	Pulse **Salir** para salir del asistente sin guardar los cambios.

3.3.3 OTIST

La siguiente pantalla permite habilitar la funcionalidad OTIST. Este funcionalidad permite al gateway asignar a los clientes inalámbricos tanto el SSID como la encriptación WEP ó WPA-PSK. El cliente inalámbrico debe igualmente soportar el OTIST y tenerlo habilitado. Consulta la sección 4.5 para más información.

Figura 18 OTIST



La siguiente tabla describe las etiquetas de esta pantalla.

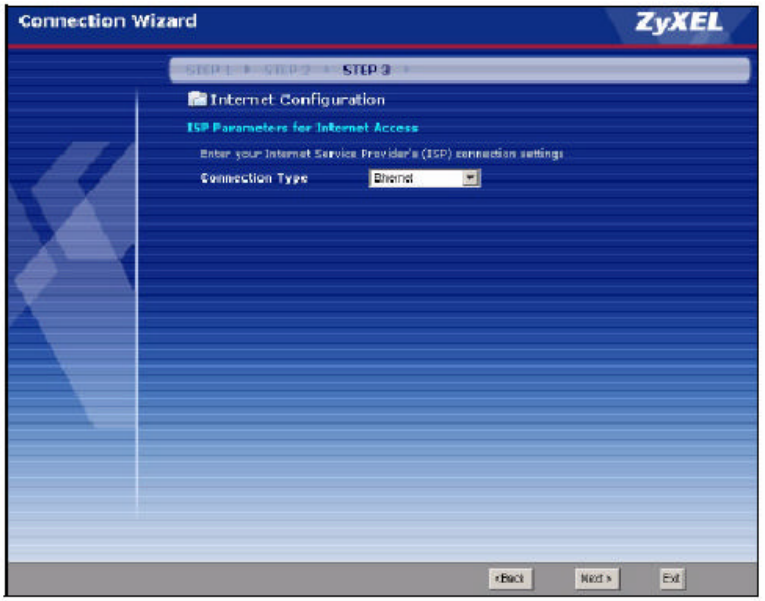
Tabla 12 OTIST

ETIQUETA	DESCRIPCIÓN
¿Desea habilitar OTIST?	Seleccione Sí y pulse Siguiente para proceder con el asistente de configuración para habilitar el OTIST sólo cuando pulse Siguiente para seguir con la siguiente pantalla.
Clave de Configuración	La clave OTIST por defecto es "01234567". La clave puede ser modificada a través del configurador web. Asegúrese de configurar la misma clave OTIST tanto en el gateway como en los clientes inalámbricos.
Atrás	Pulse **Atrás** para mostrar la pantalla anterior.
Siguiente	Pulse **Siguiente** para pasar a la siguiente pantalla.
Salir	Pulse **Salir** para salir del asistente sin guardar los cambios.

3.4 Asistente de Conexión : PASO 3: Configuración de Internet

El gateway P320W ofrece tres diferentes tipos de conexiones a Internet. Estas son Ethernet, PPP sobre Ethernet ó PPTP.

Figura 19 Asistente de conexión: PASO 3: Tipo de Conexión WAN



La siguiente tabla describe las etiquetas de esta pantalla.

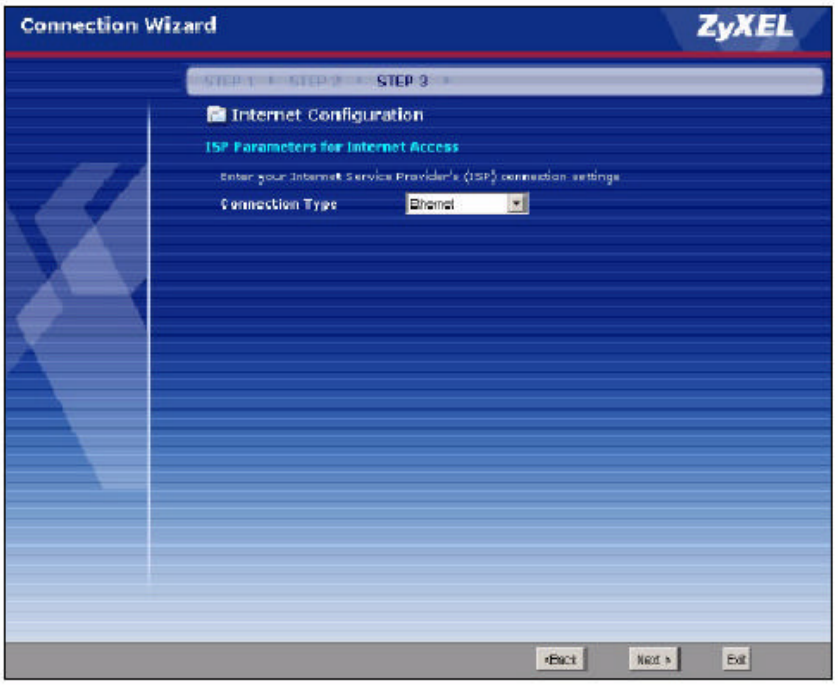
Tabla 13 Asistente de conexión: PASO 3: Tipo de conexión WAN

ETIQUETA	DESCRIPCIÓN
Ethernet	Seleccione Ethernet cuando el puerto WAN este utilizando una conexión Ethernet.
PPPoE	Seleccione PPP sobre Ethernet para una conexión telefónica a redes. Si su ISP le proporciona una dirección IP y una máscara de subred, entonces seleccione PPTP.
PPTP	Seleccione PPTP para el establecimiento de una conexión telefónica a redes.

3.4.1 Conexión Ethernet

Seleccione **Ethernet** cuando el puerto WAN utilice una conexión Ethernet tradicional.

Figura 20 Conexión Ethernet



3.4.2 Conexión PPPoE

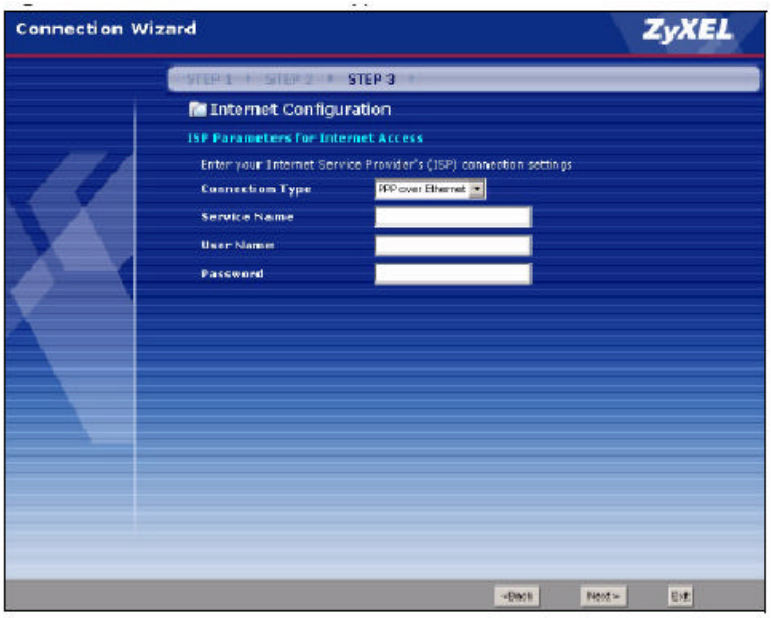
La encapsulación PPPoE funciona como una conexión telefónica a redes. La encapsulación PPPoE ofrece un acceso y un método de autenticación que funciona con un sistema de control de acceso existente (Por ejemplo, RADIUS).

Uno de los beneficios del PPPoE es la habilidad de permitir a los usuarios el acceso a diferentes servicios de red, una función definida como selección del servicio dinámico. Este posibilita al proveedor del servicio para crear y ofrecer de forma más sencilla, nuevos servicios IP para usuarios específicos.

Operacionalmente, el uso del PPPoE ahorra esfuerzos significativos tanto para el usuario final como para el proveedor del servicio.

Mediante la implementación del PPPoE en el gateway P320W (en lugar de en cada ordenador), los ordenadores de la LAN no necesitan tener instalado ningún software de cliente PPPoE, dado que el gateway realiza esta tarea. Además, con el NAT, todos los ordenadores de la LAN dispondrán del acceso a Internet.

Figura 21 Conexión PPPoE



La siguiente tabla describa las etiquetas de la siguiente pantalla.

Tabla 14 Conexión PPPoE

ETIQUETA	DESCRIPCIÓN
Parámetros ISP para el acceso a internet	
Nombre del servicio	Introduzca el nombre de su proveedor de servicio.
Nombre de usuario	Introduzca el nombre de usuario facilitado por su ISP.
Contraseña	Introduzca la contraseña asociada con el nombre de usuario anterior.
Siguiente	Pulse **Siguiente** para continuar.
Atrás	Pulse **Atrás** para volver a la pantalla anterior.
Salir	Pulse **Salir** para salir del asistente sin guardar los cambios.

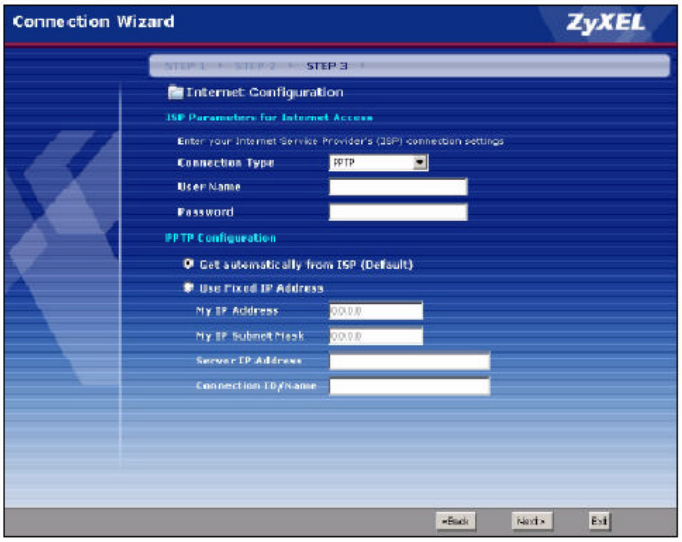
3.4.3 Conexión PPTP

El protocolo PPTP es un protocolo de red que habilita la transferencia de datos desde un cliente remoto a un servidor privado, cuando una VPN utilizando la red TCP/IP.

PPTP facilita redes privadas virtuales multiprotocolo sobre redes públicas, como Internet.

Nota: El P320W soporta una conexión con un servidor PPTP simultáneamente.

Figura 22 Conexión PPTP



La siguiente tabla describe las etiquetas de esta pantalla.

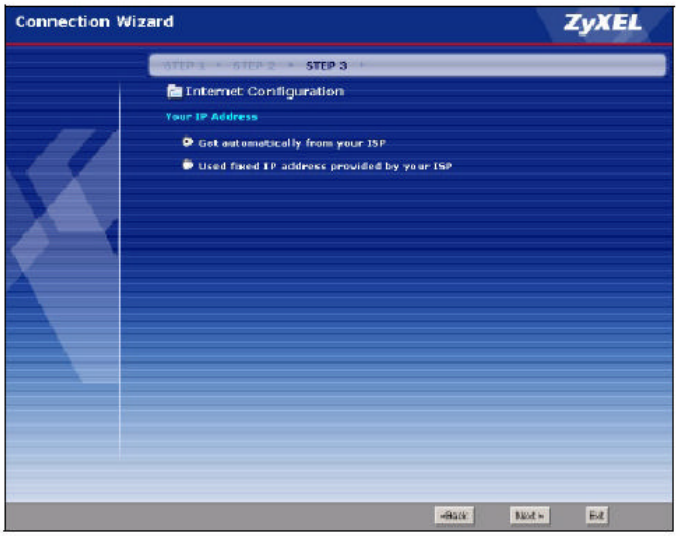
Tabla 15 Conexión PPTP

ETIQUETA	DESCRIPCIÓN
Parámetros ISP para el acceso a internet	
Nombre de usuario	Introduzca el nombre de usuario proporcionado por su ISP.
Contraseña	Introduzca la contraseña asociada con el nombre de usuario anterior.
Configuración PPTP	
Obtención automática desde el ISP	Seleccione esta opción si su ISP no le ha proporcionado ninguna dirección IP
Utilizar dirección IP estática	Seleccione esta opción si su ISP le ha proporcionado una dirección IP estática
Mi dirección IP	Introduzca la dirección IP estática asignada por su ISP.
Mi máscara de subred	Introduzca la máscara de subred asignada por su ISP.
Dirección IP del servidor	Introduzca la dirección IP del servidor PPTP
Identificador/Nombre de Conexión	Introduzca el identificador o el nombre de la conexión en este campo. Este campo es opcional y depende de los requisitos del ISP.
Atrás	Pulse **Atrás** para volver a la pantalla anterior.
Siguiente	Pulse **Siguiente** para pasar a la siguiente pantalla.
Salir	Pulse **Salir** para salir del asistente sin guardar los cambios.

3.4.4 Dirección IP

La siguiente pantalla del asistente permite asignar una dirección IP estática o configurar una asignación dinámica de la dirección IP en función de su ISP.

Figura 23 Dirección IP



La siguiente tabla describe las etiquetas de esta pantalla.

Tabla 16 Dirección IP

ETIQUETA	DESCRIPCIÓN
Obtener automáticamente desde el ISP	Seleccione esta opción si su ISP no le asigna una dirección IP estática. Esta será la opción por defecto.
Utilizar una dirección IP estática proporcionada por su ISP	Seleccione esta opción si su ISP le asigna una dirección IP. La dirección IP fija deberá estar dentro de la misma subred de su router o módem de acceso.
Atrás	Pulse **Atrás** para volver a la pantalla anterior.
Siguiente	Pulse **Siguiente** para continuar.
Salir	Pulse **Salir** para salir del asistente sin guardar los cambios.

3.4.5 Dirección MAC

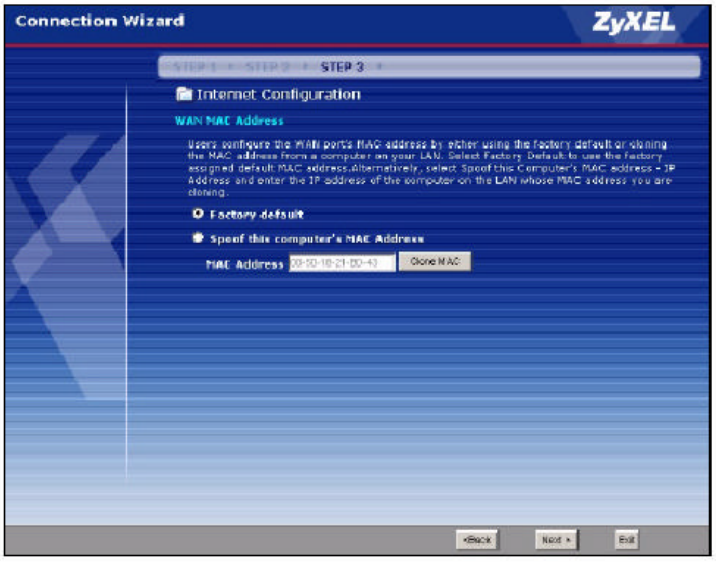
Cada dispositivo Ethernet tiene una dirección MAC única. La dirección MAC es asignada en la fabricación y consiste un seis pares de caracteres hexadecimales, por ejemplo, 00-A0-C5-00-00-02.

Tabla 17 Ejemplo de Propiedades de red para servidores en LAN con direcciones IP fijas

Escoger una dirección IP	192.168.1.2-192.168.1.32; 192.168.1.65-192.168.1.254
Máscara de subred	255.255.255.0
Puerta de enlace predeterminada (o ruta por defecto)	192.168.1.1 (dirección IP del P320W)

Esta pantalla permite al usuario configurar la dirección MAC del puerto WAN utilizando los parámetros por defecto.

Figura 24 Dirección MAC



La siguiente tabla describe los campos de esta pantalla.

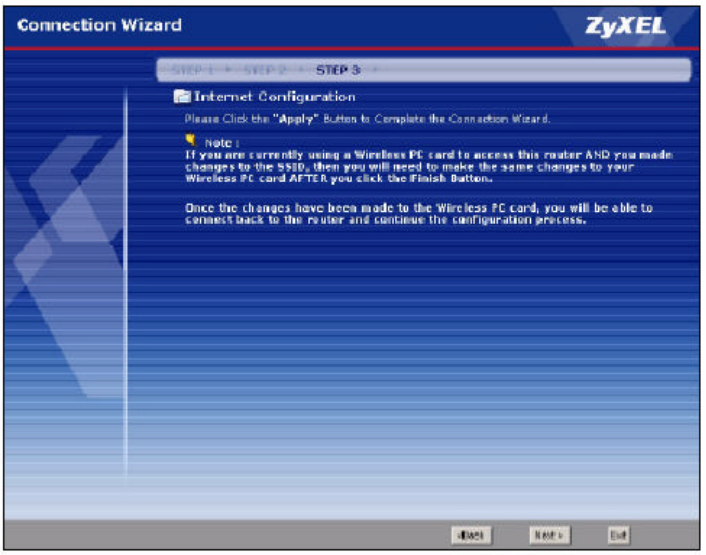
Tabla 18 Dirección MAC

ETIQUETA	DESCRIPCIÓN
Parámetros por defecto	Seleccione Parámetros por defecto para utilizar los parámetros por defecto asignando la dirección MAC por defecto.
Utilizar la dirección MAC de un ordenador	Seleccione esta opción y pulse Clonar MAC para utilizar la dirección MAC en este campo. Una vez se haya configurado satisfactoriamente, la dirección será copiada al fichero de configuración del P320W. El mismo no se modificará a menos que se modifiquen los parámetros o se actualice el fichero de configuración.
Dirección MAC	Introduzca la dirección MAC del ordenador de la LAN cuya dirección MAC se quiere clonar.
Atrás	Pulse **Atrás** para volver a la pantalla anterior.
Siguiente	Pulse **Siguiente** para pasar a la siguiente pantalla.
Salir	Pulse **Salir** para salir del asistente sin guardar los cambios.

3.4.6 Completar el asistente de configuración

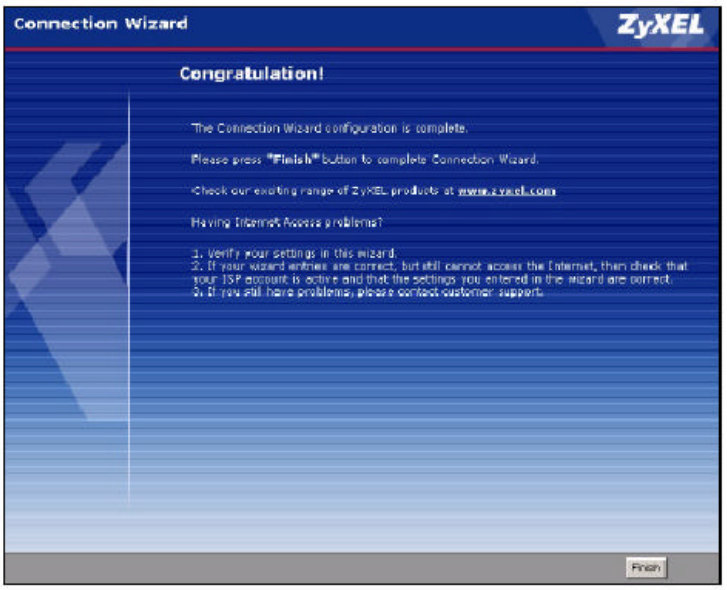
Siga las instrucciones de la pantalla y pulse **Siguiente.**

Figura 25 Completar el asistente de configuración



Pulse Finalizar para completar el asistente de configuración y guardar los parámetros.

Figura 26 Asistente de Configuración



Ya dispone de su gateway configurado y funcional en su entorno de red para acceder a Internet

CAPÍTULO 4: LAN INALÁMBRICA

Este capítulo describe como configurar la red LAN inalámbrica

4.1 Introducción

Una LAN inalámbrica puede estar formada por algo tan simple como dos ordenadores con adaptadores inalámbricos formando una red peer-to-peer o tan compleja como un determinado número de ordenadores con adaptadores inalámbricos comunicados mediante puntos de acceso con la red cableada.

4.2 Descripción Seguridad Inalámbrica

La seguridad inalámbrica es vital para una red inalámbrica para proteger la comunicación entre las estaciones inalámbricas, puntos de acceso y red cableada.
Los métodos de seguridad inalámbrica disponible en su gateway son la encriptación de datos, la autenticación de clientes inalámbricos, la restricción de acceso por dirección MAC y la ocultación de la identidad del router.

4.2.1 Encriptación

• Utilice la seguridad WPA si sus clientes inalámbricos son compatibles con WPA y dispone de servidor RADIUS. WPA proporciona autenticación de usuario y encriptación de datos mejorada sobre la encriptación WEP.
• Utilice WPA-PSK si sus clientes inalámbricos son compatibles con WPA pero no dispone de servidor RADIUS.
• Si sus clientes inalámbricos no son compatibles con WPA, entonces utilice encriptación WEP. Puede introducir una clave para automáticamente generar las claves de 64-bits ó 128-bits o teclear manualmente las claves WEP de 64 ó 128 bits.

4.2.2 Autenticación

El modo WPA utiliza la autenticación de usuario y es posible configurar IEEE 802.1x para utilizar un servidor RADIUS para autenticar a los clientes inalámbricos antes de unirse a la red.
• Utilizar la autenticación RADIUS si dispone de servidor RADIUS.

4.2.3 Acceso restringido

La pantalla del **Filtrado MAC** permite configurar el punto de acceso para permitir el acceso a determinados dispositivos (**Permitir**) o excluirlos del acceso al mismo (**Denegar**).

4.2.4 Ocultar la Identidad del Gateway

Si se oculta el SSID del gateway, entonces el P320W no podrá ser visto cuando una estación inalámbrica realice una búsqueda de estación.

4.2.5 Utilización de OTIST

En una red inalámbrica, los clientes inalámbricos deben tener el mismo valor de SSID y de seguridad que el punto de acceso para asociarse con él. Tradicionalmente esto significa que es necesario configurar los parámetros en el punto de acceso y después configurarlas manualmente de forma idéntica en cada cliente inalámbrico.

La funcionalidad OTIST permite transferir el SSID y los parámetros de seguridad WEP ó WPA-PSK de su punto de acceso a los clientes inalámbricos que soporten OTIST y que se encuentren dentro de la zona de cobertura. También puede configurar el punto de acceso para que genere una clave WPA-PSK automáticamente si no se configura ninguna de forma manual.

Nota: OTIST reemplaza los parámetros inalámbricos pre-configurados en los clientes inalámbricos.

4.3 Configurando la LAN inalámbrica

1. Configure el SSID y el modo de seguridad en la pantalla Inalámbrica. Si configura WEP, no podrá configurar WPA ni WPA-PSK.
2. Utilice la pantalla de Filtrado MAC para restringir el acceso a la red en base a la dirección MAC.
3. Si tiene clientes con OTIST habilitado, configure OTIST en la pantalla OTIST. El OTIST transfiere los parámetros SSID y WEP ó WPA-PSK a los clientes inalámbricos.

La siguiente figura muestra la eficacia relativa de los métodos de seguridad disponibles en su P320W.

Tabla 19 Niveles de seguridad inalámbrico

Nivel de Seguridad	Tipo de seguridad
Seguridad más baja	SSID único (defecto)
	SSID único, ocultando el SSID
	Filtrado por direccionamiento MAC
	Encriptación WEP
	IEEE 802.1x EAP con autenticación servidor RADIUS
Seguridad más alta	Wi-Fi Protected Access (WPA)

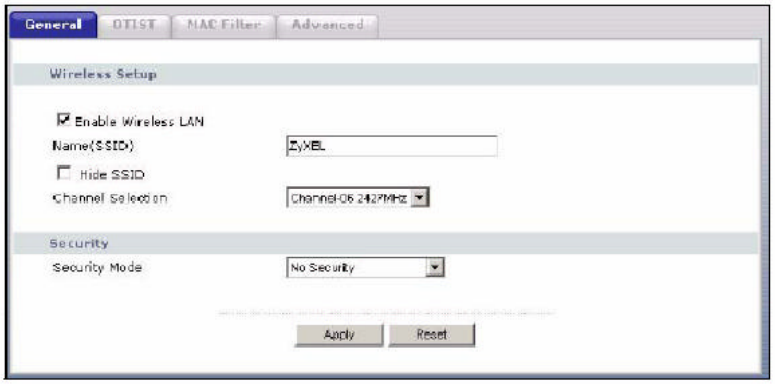
Nota: Debe habilitar los mismos parámetros de seguridad en su router y en sus clientes inalámbricos para permitir que los clientes se asocien con él.

4.4 Pantalla general de la LAN inalámbrica

Nota: Si está configurando su router desde un ordenador conectado a su red inalámbrica y modifica los valores del SSID ó de encriptación WEP, perderá la conexión inalámbrica cuando pulse el botón **Aplicar** para confirmar los cambios. En ese momento deberá modificar los parámetros inalámbricos de su ordenador para hacerlos coincidir con los nuevos configurados en su gateway.

Pulse el enlace **LAN inalámbrica** bajo las opciones de **Red** para abrir la pantalla **General**.

Figura 27 Red inalámbrica: General



La siguiente tabla describe las etiquetas de esta pantalla.

Tabla 20 Red inalámbrica: General

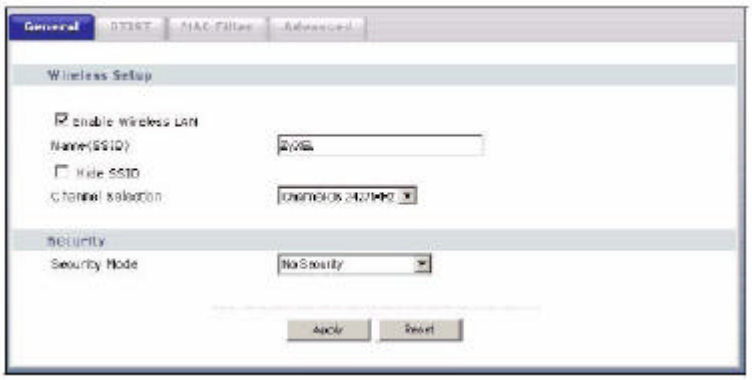
ETIQUETA	DESCRIPCIÓN
Habilitar LAN Inalámbrica	Pulse sobre esta casilla para activar la red inalámbrica
Nombre (SSID)	El valor del SSID identifica el nombre de la red inalámbrica con el que se asocian los clientes inalámbricos. Introduzca un nombre descriptivo (de hasta 32 caracteres) para la LAN inalámbrica.
Ocultar el SSID	Seleccione esta casilla para ocultar el SSID de manera que las estaciones inalámbricas no puedan obtener el SSID al realizar búsquedas pasivas de estaciones.
Selección de canal	Configure un canal operativo dependiendo de su región. Seleccione un canal de la lista desplegable.
Aplicar	Pulse **Aplicar** para guardar los cambios realizados.
Resetear	Pulse **Resetear** para cargar los parámetros de configuración originales en este pantalla.

4.4.1 Sin Seguridad

Seleccione **Sin Seguridad** para permitir a las estaciones inalámbricas el comunicarse con los puntos de acceso sin ningún tipo de encriptación.

Nota: Si no habilita ningún tipo de seguridad en su P320W, su red será accesible a cualquier dispositivo de red dentro de su rango de cobertura.

Figura 28 Red inalámbrica : Sin seguridad



La siguiente tabla describe las etiquetas dentro de esta pantalla.

Tabla 21 Red inalámbrica : Sin seguridad

ETIQUETA	DESCRIPCIÓN
Modo de seguridad	Seleccione **Sin seguridad** de la lista desplegable.
Aplicar	Pulse **Aplicar** para guardar los cambios.
Resetear	Pulse **Resetear** para cargar los parámetros previos de configuración.

4.4.2 Encriptación WEP

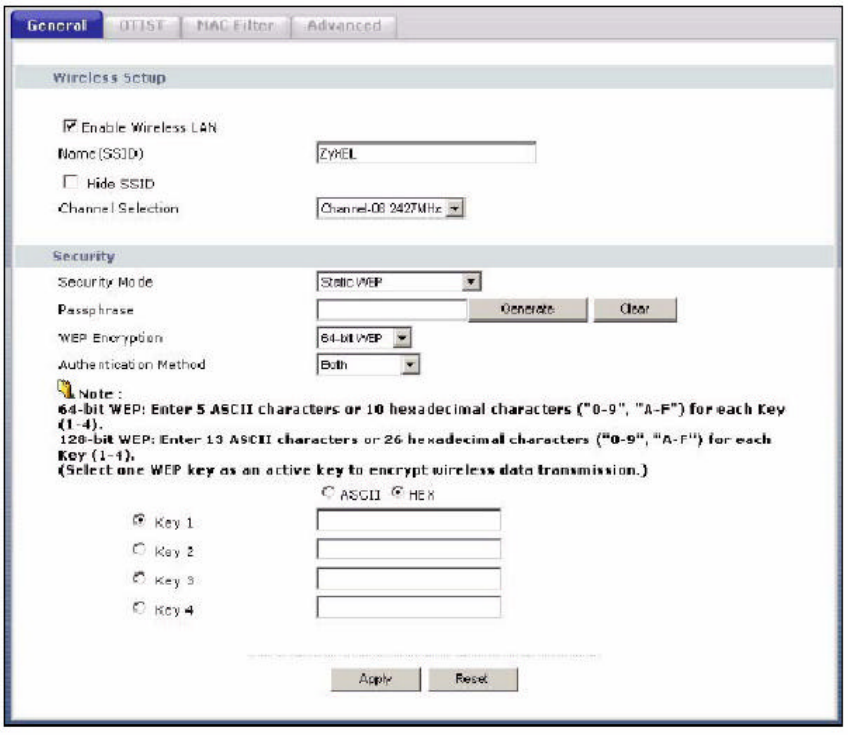
La encriptación WEP protege los datos transmitidos entre las estaciones inalámbricas y los puntos de acceso para mantener la privacidad de las comunicaciones de red. Se protegen tanto las comunicaciones unicast como multicast dentro de una red. Tanto las estaciones inalámbricas como los puntos de acceso deben de utilizar la misma clave WEP.

El P320W permite configurar hasta cuatro claves de 64 ó 128 bits pero únicamente una de ellas puede ser utilizar.

Para configurar y habilitar la encriptación WEP; pulse sobre **Red Inalámbrica** y **Wireless** para mostrar la pantalla **General**.

Seleccione **WEP Estática** de la lista desplegable de **Modo de Seguridad**.

Figura 29 Red inalámbrica : Encriptación WEP Estática



La siguiente tabla describe las etiquetas de seguridad LAN de esta pantalla.

Tabla 22 Red inalámbrica: Encriptación WEP estática

ETIQUETA	DESCRIPCIÓN
Clave	Introduzca una clave (de hasta 32 caracteres) y pulse sobre **Generar**. El P320W generará automáticamente los cuatro claves WEP.
Generar	Tras introducir la clave, pulse sobre **Generar** para que el router genere automáticamente las cuatro claves WEP.
Borrar	Pulse sobre **Borrar** para descartar la clave configurada en el router y las claves WEP generadas automáticamente e introducir las mismas de forma manual
Encriptación WEP	Seleccione **64-bit WEP** ó **128-bit WEP** para habilitar la encriptación de datos
Método de autenticación	Seleccione **Auto, Abierto** ó **Compartido** de la lista desplegable.
ASCII	Seleccione esta opción para introducir las claves WEP en formato de caracteres ASCII.
HEX	Seleccione esta opción para introducir las claves WEP en formato hexadecimal. El valor "0x" que identifica una clave hexadecimal se introducirá de forma automática.
Clave 1 a 4	Las claves WEP se utilizan para encriptar los datos. Tanto el router como los clientes inalámbricos deberán utilizar las mismas claves para la transmisión de datos. Si selecciona el modo 64-bit WEP, introduzca 5 caracteres ASCII ó 10 caracteres hexadecimales. Si selecciona el modo 128-bit WEP, introduzca 13 caracteres ASCII ó 26 caracteres hexadecimales. Deberá introducir al menos una clave, únicamente una clave estará activa en cada momento. La clave por defecto es la 1.
Aplicar	Pulse Aplicar para guardar los cambios.
Resetear	Pulse Resetear para cargar los parámetros previos en esta pantalla.

4.4.3 Introducción al WPA

Wi-Fi Protected Access (WPA) es un subconjunto del estándar IEEE 802.1i. WPA es un mecanismo de protección superior al WEP dado que proporciona autenticación de usuario y una encriptación de datos mejorada.

Si tanto el punto de acceso como los clientes inalámbricos soportan WPA y dispone de un servidor RADIUS, utilice WPA para fortalecer la encriptación de datos. Si no dispone de servidor RADIUS externo, deberá utilizar WPA-PSK que únicamente requiere el introducir una clave en cada punto de acceso y cliente inalámbrico. Si las contraseñas coinciden, al cliente inalámbrico se le permitirá el acceso a la red WLAN.

4.4.4 Ejemplo de Aplicación WPA-PSK

Una aplicación WPA-PSK tiene en cuenta los siguientes aspectos:

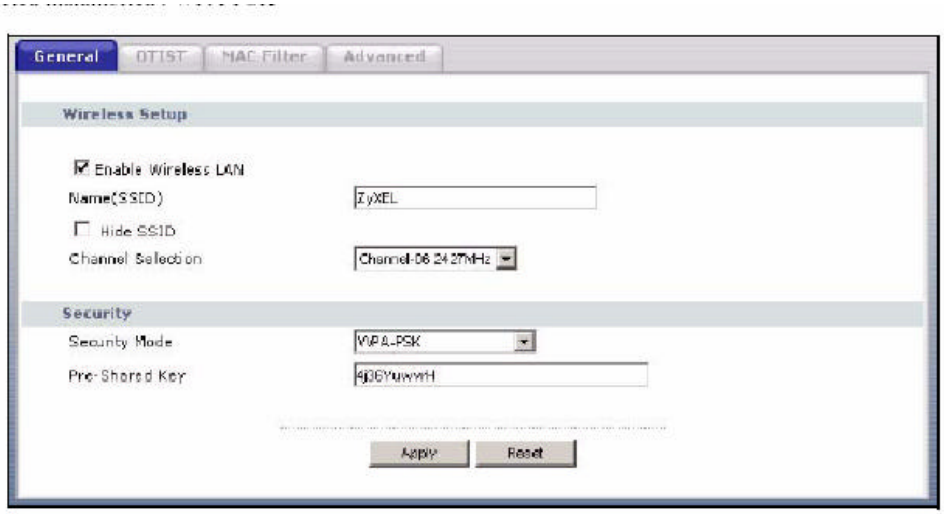
1. En primer lugar introducir una clave idéntica tanto en el punto de acceso como en los clientes inalámbricos. La clave (PSK) debe tener entre 8 y 63 caracteres (incluyendo espacios y símbolos)
2. El punto de acceso comprueba la clave de cada cliente inalámbrico y únicamente se permite el unirse a la red si la clave coincide.
3. El punto de acceso genera y distribuye las claves a los clientes inalámbricos.
4. El punto de acceso y los clientes inalámbricos utilizan el proceso de encriptacion TKIP para encriptar los datos intercambiados entre ellos.

Figura 30 Autenticación WPA-PSK

4.4.5 Pantalla de Autenticación WPA-PSK

Para configurar y habilitar la autenticación WPA-PSK; pulse sobre el enlace **Red Inalámbrica** bajo la opción de **Red** para mostrar la pantalla **General**. Seleccione **WPA-PSK** de la lista **Modo de Seguridad**.

Figura 31 Red inalámbrica : WPA-PSK



La siguiente tabla describe las etiquetas dentro de esta pantalla.

Tabla 23 Red inalámbrica : WPA-PSK

ETIQUETA	DESCRIPCIÓN
Clave pre-compartida	Los mecanismos de encriptación utilizados por **WPA** y **WPA-PSK** son idénticos. La única diferencia entre ellos es que WPA-PSK utiliza una clave simple, en lugar de credenciales específicas de usuario. Introduzca la clave de entre 8 y 63 caracteres ASCII (identificando entre mayúsculas y minúsculas).
Aplicar	Pulse **Aplicar** para guardar los cambios
Resetear	Pulse **Resetear** para volver a cargar los parámetros previos en esta pantalla.

4.4.6 Ejemplo de Aplicación WPA con RADIUS

Es necesario disponer de la dirección IP del servidor RADIUS, el número de puerto (por defecto 1812), y la clave utilizada por el RADIUS. Un ejemplo de aplicación WPA con un servidor RADIUS externo se muestra a continuación.

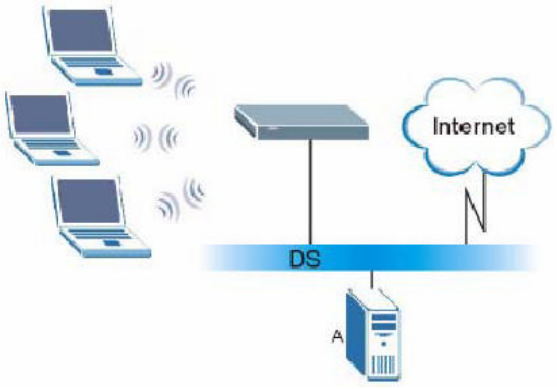
“A” es el servidor RADIUS. “DS” es el sistema de distribución.

1. El punto de acceso transfiere la petición de autenticación del cliente inalámbrico al servidor RADIUS.

2. El servidor RADIUS comprueba la identificación de usuario con su base de datos y permite o deniega el acceso a la red.

3. El servidor RADIUS distribuye una clave PMK (Pairwise Master Key) al punto de acceso que seguidamente configura una jerarquía de claves y de sistema de gestión, utilizando la clave pair-wise para generar dinámicamente unas claves únicas para la encriptación de datos para encriptar cada paquete intercambiado entre el punto de acceso y los clientes inalámbricos.

Figura 32 Ejemplo de Aplicación WPA con RADIUS



4.4.7 Suplicantes de clientes inalámbricos WPA

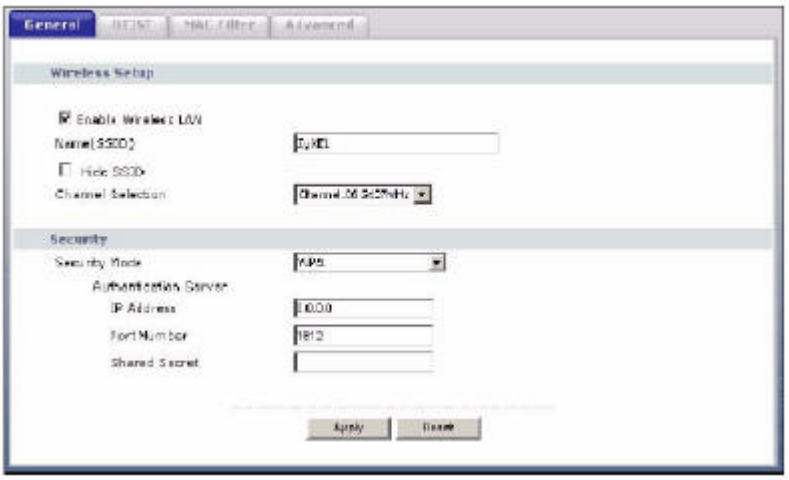
Un suplicante de un cliente inalámbrico es un software ejecutándose en un sistema operativo que posibilita a un cliente inalámbrico el hacer uso del modo WPA.

Windows XP proporciona una utilidad gratuita que incluye capacidades WPA dentro del cliente inalámbrico “Zero Configuration” soportado por dicha versión del sistema operativo. Sin embargo, es necesario utilizar dicho sistema Windows XP para hacer uso de dicha utilidad.

4.4.8 Pantalla de Autenticación WPA

Para configurar y habilitar la autenticación WPA; pulse sobre el enlace **Red Inalámbrica** bajo la opción de **Red** para mostrar la pantalla **General**. Seleccione **WPA** de la lista **Modo de Seguridad**.

Figura 33 Red inalámbrica: WPA



La siguiente figura describe las etiquetas de esta pantalla.

Tabla 24 Red inalámbrica: WPA

ETIQUETA	DESCRIPCIÓN
Servidor de autenticación	
Dirección IP	Introduzca la dirección IP del servidor de autenticación externo.
Número de puerto	Introduzca el número de puerto del servidor de autenticación externo. El puerto por defecto es el 1812. No será necesario el modificar este valor a menos que su administrador de red se lo indicase.
Clave compartida	Introduzca una contraseña (de hasta 31 caracteres alfanuméricos) como clave para ser compartida entre el servidor de autenticación externo y el P320W. La clave debe ser la misma tanto en el servidor externo como en el gateway. La calve no es enviada a través de la red.
Aplicar	Pulse **Aplicar** para guardar los cambios introducidos.
Resetear	Pulse **Resetear** para cargar los parámetros previos en esta pantalla.

4.4.9 Descripción IEEE 802.1x

Deberá seguir las siguientes indicaciones para configurar una autenticación IEEE 802.1x.

• Un ordenador equipado con un adaptador IEEE 802.11 a/b/g con un navegador web (con JavaScript habilitado) y/o telnet.

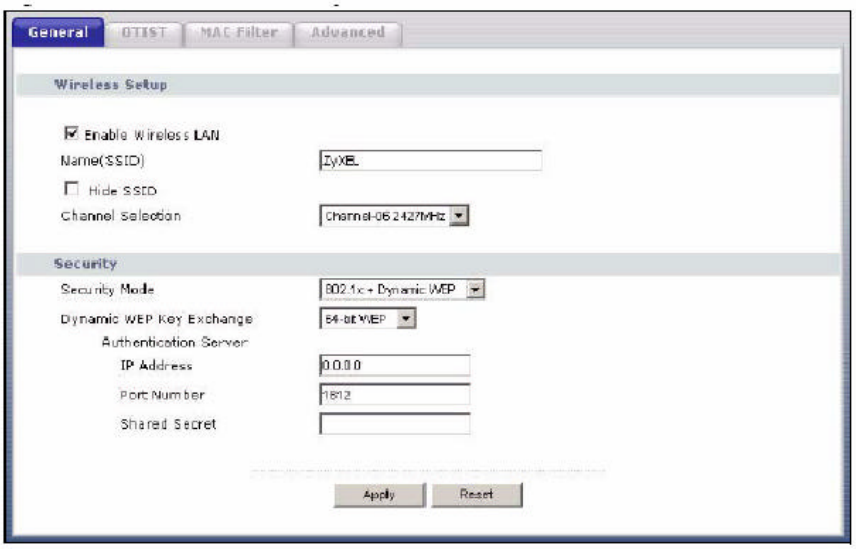
• El equipo debe estar ejecutando un software compatible con IEEE 802.1x.

• Un servidor RADIUS opcional para autenticación y contabilidad de usuarios.

4.4.10 Pantalla IEEE 802.1x e intercambio de clave WEP dinámica

Para configurar y habilitar el modo 802.1x con intercambio de WEP dinámica; pulse sobre **Red inalámbrica** bajo la opción **Red** para mostrar la pantalla **General**. Seleccione **802.1x + WEP dinámica** de la lista **Modo de Seguridad**.

Figura 34 Red inalámbrica: 802.1x y WEP dinámica



La siguiente tabla describe las etiquetas de esta pantalla.

Tabla 25 Red inalámbrica: 802.1x y WEP dinámica

ETIQUETA	DESCRIPCIÓN
Intercambio de clave WEP dinámica	Seleccione 64-bit WEP ó 128-bit WEP para habilitar la encriptación de datos. Hasta 32 estaciones podrán acceder al gateway cuando se configura el intercambio dinámico de clave WEP.
Servidor de Autenticación	
Dirección IP	Introduzca la dirección IP del servidor externo de autenticación.
Número de puerto	Introduzca el número de puerto del servidor de autenticación externo. El puerto por defecto es el 1812.
Clave secreta	Introduzca una contraseña (de hasta 31 caracteres) como la clave a ser compartida entre el servidor externo y el punto de acceso. La clave debe ser la misma tanto en el servidor de autenticación como en el P320W.
Aplicar	Pulse **Aplicar** para guardar los cambios.
Resetear	Pulse **Resetear** para cargar los parámetros previos para esta pantall.a

4.5 OTIST

La funcionalidad OTIST (One-Touch Intelligent Security Technology) permite al P320W configurar las estaciones inalámbricas con los mismos parámetros configurados en el gateway.

Nota: Los clientes inalámbricos deben soportar OTIST y tener dicha funcionalidad habilitada.

A continuación se muestran los parámetros inalámbricos que el router asigna a los clientes inalámbricos si el OTIST está habilitado en ambos dispositivos y la clave OTIST coincide.

• SSID

• Seguridad (WEP ó WPA-PSK)

Nota: Esto reemplazará los parámetros inalámbricos pre-configurados en los clientes inalámbricos.

4.5.1 Habilitando OTIST

Es necesario habilitar la función OTIST tanto en el punto de acceso como en el cliente inalámbrico antes de comenzar a transferir los parámetros inalámbricos.

Nota: El punto de acceso y los clientes inalámbricos deben utilizar la misma **Clave de Configuración**.

4.5.1.1 Punto de Acceso

Es posible habilitar el OTIST mediante la utilización del botón Reset o del configurador Web.

4.5.1.1.1 Botón de reset

Si se utiliza el botón de **Reset**, el valor por defecto (01234567) o el valor previamente guardado (a través del configurador web) en la **Clave de Configuración** será el utilizado para encriptar los parámetros que se desean transferir.

Mantenga pulsado el botón de **Reset** durante uno o dos segundos.

Nota: Si mantiene pulsado el botón de **Reset** demasiado tiempo, el dispositivo se reseteará a los parámetros por defecto.

4.5.1.1.2 Configurador Web

Pulse sobre **Red Inalámbrica** bajo el enlace **Red** y a continuación en la pestaña **OTIST**. Le aparecerá una pantalla como la siguiente.

Figura 35 Red inalámbrica : OTIST

La siguiente tabla describe las etiquetas de esta pantalla.

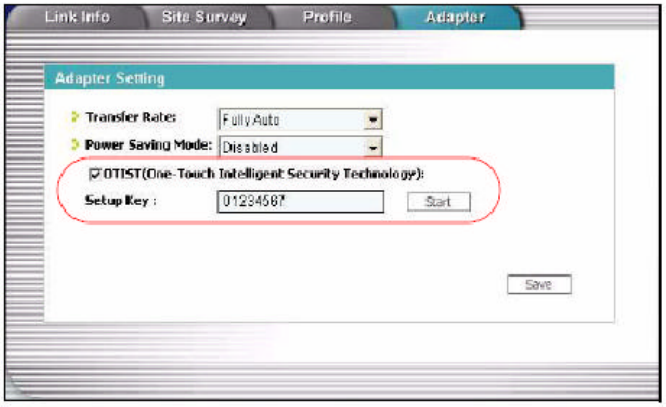
Tabla 26 Red inalámbrica: OTIST

ETIQUETA	DESCRIPCIÓN
Clave de Configuración	Introduzca la clave de configuración OTIST de 8 caracteres. La clave por defecto es "01234567". Nota : Si modifica esta clave en el punto de acceso, deberá hacerlo también en los clientes inalámbricos.
Sí	Seleccione esta casilla para que la función OTIST genere automáticamente una clave WPA-PSK. Si configura de forma manual una clave WEP y esta casilla está activada, entonces se utilizará la clave configurada manualmente. Si desea configurar su propia clave WPA-PSK y que la función OTIST utilice esa WPA-PSK, entonces deberá: • Configurar una clave WPA-PSK en la pantalla **General**. • Desmarcar esta casilla en la pantalla **OTIST** y pulsar **Aplicar**. Si desea que el sistema OTIST genere una clave WPA-PSK automáticamente, se deberá: • Cambiar la seguridad a **Sin seguridad** en la pantalla **General**. • Marcar la casilla **Sí** en esta pantalla **OTIST** y pulsar **Aplicar**. • La pantalla General mostrará una clave WPA-PSK autogenerada, configurando el punto de acceso en modo WPA-PSK. Los parámetros de seguridad WPA-PSK son asignados a los clientes inalámbricos cuando OTIST es ejecutado.
Comenzar	Pulse sobre Comenzar para encriptar los datos inalámbricos utilizando la clave de configuración y posibilitando al P320W el configurar en las estaciones inalámbricas los mismos parámetros inalámbricos que los utilizados por él mismo. Será necesario el activar y lanzar el proceso OTIST en la estación inalámbrica al mismo tiempo. El proceso llevará unos 3 minutos en completarse.

4.5.1.2 Cliente inalámbrico

Inicie la utilidad ZyXEL y pulse sobre la pestaña **Adaptador (Adapter)**. Marque la casilla **OTIST**, introduzca la misma **Clave de Configuración** de su punto de acceso y pulse sobre **Guardar (Save).**

Figura 36 Pantalla de ejemplo de cliente inalámbrico con OTIST



4.5.2 Iniciando OTIST

Nota: Será necesario pulsar sobre el botón **Iniciar** dentro de la pantalla OTIST del configurador web del punto de acceso y en la pantalla **Adaptador** de los clientes inalámbricos dentro de un periodo de tiempo tres minutos. Podrá iniciar el proceso OTIST en los clientes inalámbricos y en el punto de acceso con un orden indistinto, lo único necesario es que se encuentren dentro la misma zona de cobertura y con el OTIST activado.

1. En el punto de acceso, una pantalla popup del configurador web indicará los parámetros de seguridad que serán transferidos. Tras revisar estos parámetros, pulse OK.

Figura 37 Parámetros de Seguridad

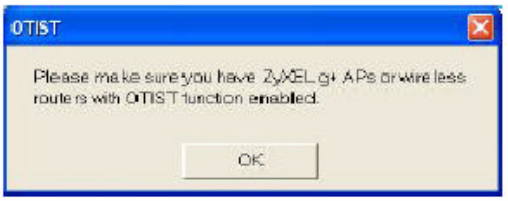
2. Esta pantalla aparecerá mientras que los parámetros OTIST son transferidos. Se cerrará cuando la transferencia se complete.

Figura 38 OTIST en progreso (punto de acceso)

Figura 39 OTIST en progreso (cliente)

3. En el cliente inalámbrico, se mostrará la siguiente pantalla si no puede detectar ningún punto de acceso con OTIST habilitado (con la misma **Clave de Configuración**). Pulse **OK** para volver a la pantalla principal de configuración de la utilidad ZyXEL.

Figura 40 Ningún punto de acceso detectado con OTIST



4. Si existe más de un punto de acceso con OTIST habilitado dentro de la zona de cobertura del cliente, se mostrará una pantalla solicitando la selección de un punto de acceso del que obtener los parámetros de seguridad.

4.5.3 Notas sobre OTIST

1. Si habilita el OTIST en el cliente inalámbrico, se le mostrará la siguiente pantalla cada vez que inicie la utilidad.

Pulse **Yes** (Sí) para que comience la detección de punto de acceso con OTIST habilitado.

Figura 41 Comenzar OTIST?

2. Si el cliente inalámbrico con OTIST habilitado pierde la conexión inalámbrica con el punto de acceso durante más de diez segundos, entonces comenzará a buscar nuevos puntos de accesos con OTIST habilitado durante un minuto. (Si se configura de forma manual que el cliente busque nuevos puntos de acceso con OTIST habilitado, entonces no existirá ningún termporizador; pulse sobre **Cancel (Cancelar)** en la pantalla de progreso para detener la búsqueda).

3. Cuando el cliente inalámbrico detecta un punto de acceso con OTIST habilitado, aún deberá pulsar el botón Stara (Iniciar) en el configurador Web del punto de acceso o mantener pulsado el botón Reset (durante uno o dos segundos) para que el punto de acceso transfiriese los parámetros.

4. Si se modifica el SSID o las claves en el punto de acceso tras haber hecho uso del OTIST, será necesario volver a ejecutar OTIST o introducir manualmente los nuevos valores en los clientes inalámbricos.

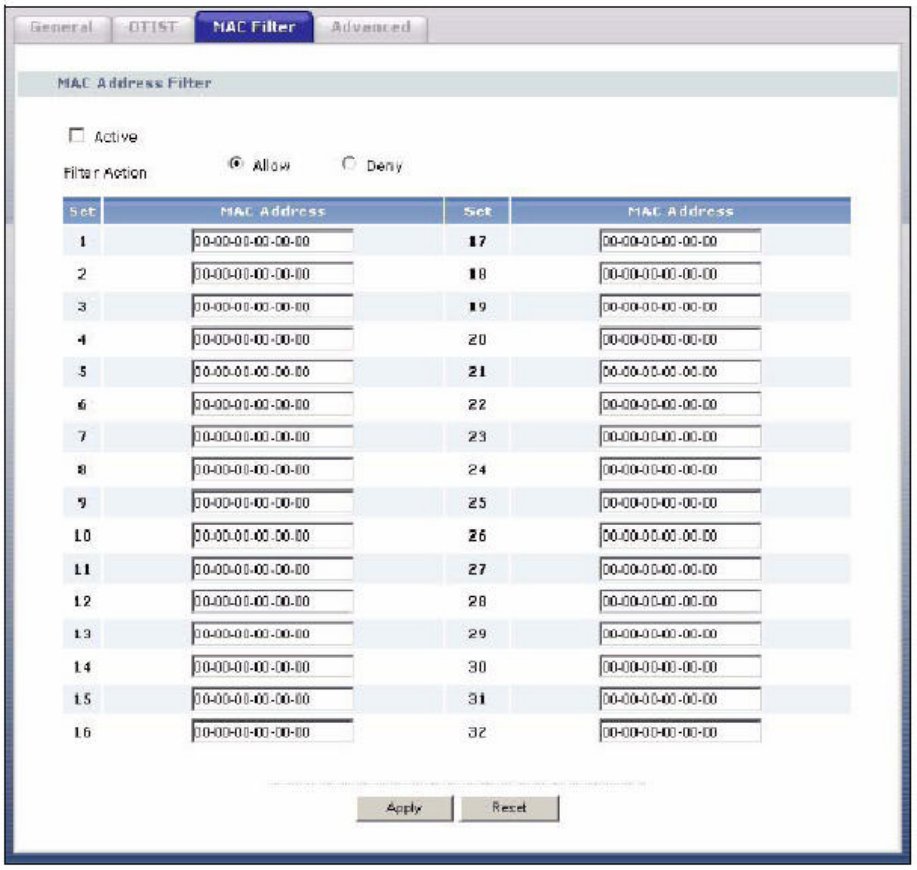
5. Si se configura OTIST para que genere una clave WPA-PSK, esta clave cambiará cada vez que se ejecute el proceso OTIST. De manera que si un nuevo cliente se asocia a la red, será necesario nuevamente ejecutar OTIST tanto en el punto de acceso como en todos los clientes inalámbricos.

4.6 Filtrado MAC

La pantalla del Filtrado MAC permite configurar el P320W para permitir (**Allow**) el acceso exclusivamente a determinadas estaciones inalámbricas (hasta 32 dispositivos) o impedir (**Deny**) que hasta 32 dispositivos puedan asociarse al P320W. Cada dispositivo Ethernet cuenta con una dirección MAC única. La dirección MAC es asignada en la fabricación y consiste en seis pares de caracteres hexadecimales, por ejemplo, 00-A0-C5-00-00-02. Será necesario conocer la dirección MAC de los dispositivos antes de configurar esta pantalla.

Para modificar los parámetros de filtrado MAC de su gateway, pulse sobre **Red inalámbrica** bajo la opción **Red** y a continuación seleccione la pestaña **Filtrado MAC**. Mostrándose la siguiente pantalla.

Figura 42 Red inalámbrica: Filtrado de dirección MAC



La siguiente tabla describe las etiquetas de esta pantalla.

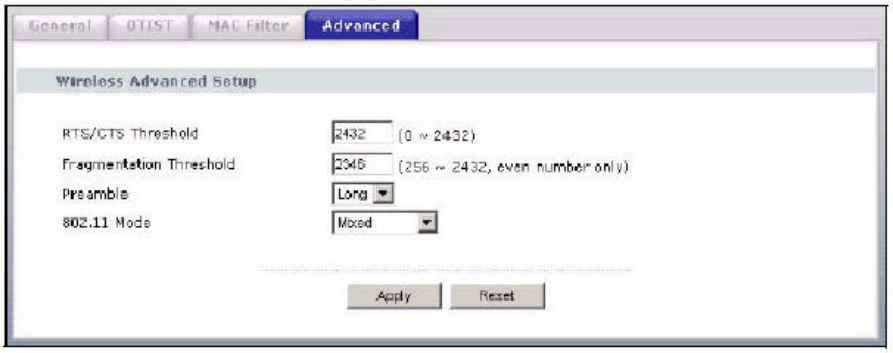
Tabla 27 Filtrado MAC

ETIQUETA	DESCRIPCIÓN
Activar	Seleccione **Sí** de la lista desplegable para habilitar el filtrado MAC
Acción de Filtrado	Defina la acción de filtrado a ejecutar para la lista de direcciones MAC en la tabla siguiente. Seleccione **Denegar** para bloquear el acceso al P320W, de manera que únicamente a las direcciones MAC que no aparezcan en la siguiente lista se les permitirá el acceso al gateway. Seleccione **Permitir** para permitir el acceso al P320W, de manera que únicamente a las direcciones MAC que aparezcan en la lista se les permitirá el acceso al gateway.
Índice	Este campo muestra el número de índice de la dirección MAC.
Dirección MAC	Introduzca las direcciones MAC de las estaciones inalámbricas a las que se les permitirá o denegará el acceso al router. Introduzca dirección MAC en el formato válido, esto es, seis pares de caracteres hexadecimales, por ejemplo, 00:A0:C5:11:22:AF
Aplicar	Pulse **Aplicar** para guardar los cambios.
Resetear	Pulse **Resetear** para colocar en los parámetros de esta pantalla la configuración previa.

4.7 Pantalla de Opciones Avanzadas de la Red Inalámbrica

Para habilitar el roaming en su P320W, pulse sobre Red inalámbrica bajo el enlace Red y a continuación seleccione la pestaña Avanzada. Se mostrará la siguiente pantalla.

Figura 43 Red inalámbrica: Avanzada



La siguiente tabla describe las etiquetas de esta pantalla.

Tabla 28 Red inalámbrica: Opciones avanzadas

ETIQUETA	DESCRIPCIÓN
Opciones avanzadas de la red inalámbrica	
Umbral RTS/CTS	Introduzca un valor entre 0 y 2432.
Umbral de Fragmentación	Este campo indica el máximo tamaño del fragmento de datos que podrá ser enviado. Introduzca un valor entre 256 y 2432.
Preámbulo	El valor del preámbulo es utilizado para indicar que existen datos que está viniendo hacia el receptor. El preámbulo corto incrementa el rendimiento dado que mientras menos tiempo se envíe el preámbulo indicará que durante más tiempo se envían datos. Todos los adaptadores IEEE 802.11b soportan preámbulo largo, aunque no todos soportan preámbulo corto. Seleccione un preámbulo **Largo** si no está seguro de que modo de preámbulo soportan sus adaptadores inalámbricos, así como para proporcionar más fiabilidad a sus comunicaciones en un entorno de redes inalámbricas congestionadas. Seleccione un preámbulo **Corto** si está seguro de que todos los adaptadores lo soportan, de manera que se proporcione mayor eficiencia a las comunicaciones. Nota : El P320W y las estaciones inalámbricas deben utilizar el mismo modo de preámbulo para comunicarse.
Modo 802.11	Seleccione **Sólo 802.11b** para permitir únicamente la asociación al gateway a dispositivos IEEE

	802.11b. Seleccione **Sólo 802.11g** para permitir únicamente la asociación al gateway a dispositivos IEEE 802.11g. Seleccione **Mixto** para permitir que tanto los dispositivos IEEE 802.11b como IEEE 802.11g puedan asociarse al gateway. La tasa de transmisión del gateway podría verse reducida.
Aplicar	Pulse **Aplicar** para guardar los cambios.
Resetear	Pulse **Resetear** para volver a cargar en los parámetros de esta pantalla los valores previos.

CAPÍTULO 5: WAN

Este capítulo describe como configurar los parámetros de WAN

5.1 Asignación de Dirección IP a la WAN

Cada ordenador en Internet debe tener una dirección IP pública única. Si sus redes están aisladas de Internet, por ejemplo, una comunicación entre dos oficinas, es posible asignar direcciones IP a los hosts sin ningún problema. Sin embargo, la IANA tiene reservadas una serie de tres bloques de direcciones IP específicas para las redes privadas.

Tabla 29 Rangos de Direcciones IP Privadas

10.0.0.0	–	10.255.255.255
172.16.0.0	–	172.31.255.255
192.168.0.0	–	192.168.255.255

Es posible obtener una dirección IP desde la IANA, desde su ISP o tenerla asignada por una red privada. Si pertenece a una pequeña empresa y su acceso a Internet es a través de un ISP, el ISP le proporcionará la dirección IP de acceso a Internet para toda su red local.

Nota: Independientemente de su situación particular, no cree una dirección IP arbitraria; siga siempre las orientaciones indicadas anteriormente. Para más información sobre la asignación de direcciones, consulta la RFC 1597 y la RFC 1466.

5.2 Dirección IP y Máscara de subred

De forma similar a la que las casas en una calle comparten un nombre común, asimismo los ordenadores en una LAN comparten un número de red común.

El número de red que obtenga dependerá de su situación particular. Si el ISP o su administrador de red asignan un bloque de direcciones IP registradas, siga sus instrucciones a la hora de configurar su dirección IP y máscara de subred.

Si el ISP no le asigna explícitamente una dirección IP, entonces lo normal es que usted disponga de un nombre de usuario y su ISP le asigne una dirección IP dinámica cuando la conexión se establezca. LA IANA (Internet Assigned Number Authority) reserva un bloque de direcciones específicas para uso privado; por favor, no utilice

otra numeración a menos que así le sea indicado. Vamos suponer que se selecciona 192.168.1.0 como el número de red; que cubre hasta 254 direcciones individuales, desde la 192.168.1.1 y la 192.168.1.254 (la 0 y la 255 están reservadas). En otras palabras, los primeros tres números especifican el número de red mientras que el último número identifica un ordenador individual dentro de la red.

Una vez decido el número de red, escoja una dirección IP sencilla de recordar, por ejemplo, 192.168.1.1, para su gateway, pero asegúrese que ningún otro dispositivo dentro de su red está utilizando esta misma dirección.

La máscara de subred especifica la posición de una dirección IP dentro de la red. El P320W calculará la máscara de subred automáticamente en base a la dirección IP introducida. No es necesario modificar la máscara de subred calculada por el P320W a menos que así le sea indicado.

5.3 Asignación de Dirección de Servidores DNS

Utilice DNS (Domain Name System) para mapear un nombre de dominio con su correspondiente dirección IP y viceversa, por ejemplo, la dirección IP de www.zyxel.com es 204.217.0.2. El servidor DNS es extremadamente importante dado que sin él, sería necesario conocer la dirección IP de un ordenador antes de acceder al mismo.

El P320W puede obtener las direcciones de los servidores DNS de las siguientes formas:

1. El ISP le informa de las direcciones de los servidores DNS, normalmente en la carta de bienvenida al contratar el servicio. Si su ISP le proporciona estas direcciones, introdúzcalas en los campos de servidor DNS dentro de la configuración del DHCP.
2. Si el ISP no le asigna ninguna información relativa a DNS, deje los campos DNS en blanco dentro de la configuración DHCP, de manera que sea el ISP el que dinámicamente asigne las direcciones IP de los servidores DNS.

5.4 Prioridad TCP/IP (Métrica)

La métrica representa el “coste de transmisión”. Un router determina la mejor ruta para la transmisión escogiendo el camino con el “coste” más bajo. El protocolo RIP utiliza el número de saltos como la medida para el coste, con un mínimo de “1” para

conexiones de red directas. El número debe encontrarse entre “1” y “15”; un valor mayor de “15” indica que el enlace está caído. A menor número, menor coste.

La métrica configura la prioridad para las rutas del P320W hacia Internet. Si existen varias rutas que tienen la misma métrica, entonces el gateway utiliza las siguientes prioridades predefinidas:

1. **WAN** : Designado por el ISP o ruta estática (consultar Capítulo 10).
2. **Redirección de Tráfico** (consultar Sección 5.9)

Por ejemplo, si la **WAN** tiene métrica “1” y la **Redirección de Tráfico** tiene métrica “2”, la conexión **WAN** actúa como ruta primaria por defecto. Si la ruta **WAN** falla al conectarse con Internet, entonces el P320W intentará la ruta marcada por la **Redirección de Tráfico**.

5.5 Dirección MAC WAN

Cada dispositivo Ethernet tiene una dirección MACC única. LA dirección MAC es asignada en la fabricación y consiste en seis pares de caracteres hexadecimales, por ejemplo, 00:A0:C5:00:00:02.

Tabla 30 Ejemplo de Propiedades de red para servidores LAN con Dirección IP Fija

Escoger una dirección IP	192.168.1.2 – 192.168.1.32; 192.168.1.65 – 192.168.1.254
Máscara de subred	255.255.255.0
Puerta de enlace predeterminada (o ruta por defecto)	192.168.1.1 (Dirección LAN P320W)

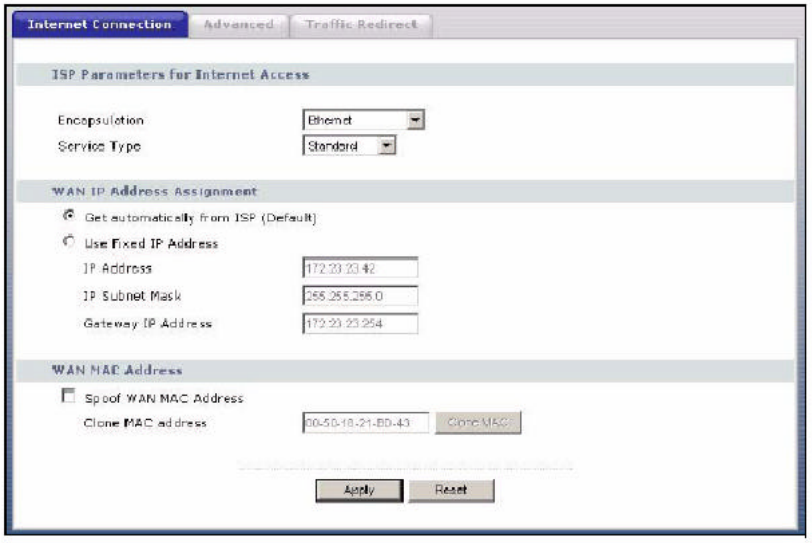
5.6 Conexión a Internet

Para modificar los valores de los parámetros IP y MAC de su gateway, pulse sobre **WAN** bajo las opciones de **Red**. La pantalla que aparecerá será diferente para cada tipo de encapsulación.

5.6.1 Encapsulación Ethernet

La pantalla que se muestra a continuación pertenece a la encapsulación **Ethernet.**

Figura 44 WAN : Encapsulación Ethernet



La siguiente tabla describe las etiquetas dentro de esta pantalla.

Tabla 31 WAN : Encapsulación Ethernet

ETIQUETA	DESCRIPCIÓN
Encapsulación	Deberá escoger la opción **Ethernet** cuando el puerto WAN sea utilizado como un puerto Ethernet normal.
Tipo de Servicio	Escoja entre **Standard, Telstra** (Método de autenticación RoadRunner Telstra), **RR-Manager** (Método de autenticación RoadRunner Manager), **RR-Toshibla** (Método de autenticación RoadRunner Toshiba) ó **Telia Login**. Los siguientes campos no aparecen para un tipo de servicio **Standard**.
Asignación de Dirección IP WAN	
Obtener automáticamente del ISP	Seleccione esta opción si su ISP no le ha proporcionado una dirección IP fija.Ésta será la opción por defecto.
Utilizar una dirección IP fija	Seleccione esta opción si su ISP le ha asignado una dirección IP fija.

Dirección IP	Introduzca la dirección IP WAN en este campo si ha seleccionado la opción Utilizar una dirección IP fija.
Máscara de subred	Introduzca la máscara de subred en este campo (si le ha sido facilitada por su ISP).
Puerta de enlace predeterminada	Introduzca la dirección de la puerta de enlace predeterminada (si le ha sido facilitada por su ISP)
Dirección MAC WAN	
Spoofing de la dirección MAC WAN	La sección de la dirección MAC permite a los usuarios el configurar la dirección MAC del puerto WAN bien utilizando la dirección por defecto o clonando la dirección MAC de un ordenador de LAN. No marcar la casilla de selección para utilizar la dirección MAC por defecto. Seleccionar esta opción y vaya sobre Clonar MAC para introducir la dirección MAC en el campo siguiente.
Clonar dirección MAC	Introducir la dirección MAC del ordenador de la LAN cuya MAC se va a clonar.
Aplicar	Pulse **Aplicar** para guardar los cambios.
Resetear	Pulse **Resetear** para volver a cargar en los parámetros de esta pantalla los valores previos.

5.6.2 Encapsulación PPPoE

El P320W soporta las conexiones PPPoE (Point-to-Point Protocol over Ethernet). Para el proveedor de servicio, el PPPoE ofrece unos métodos de acceso y autenticación que pueden funcionar con sistemas de control de acceso existentes (como RADIUS).

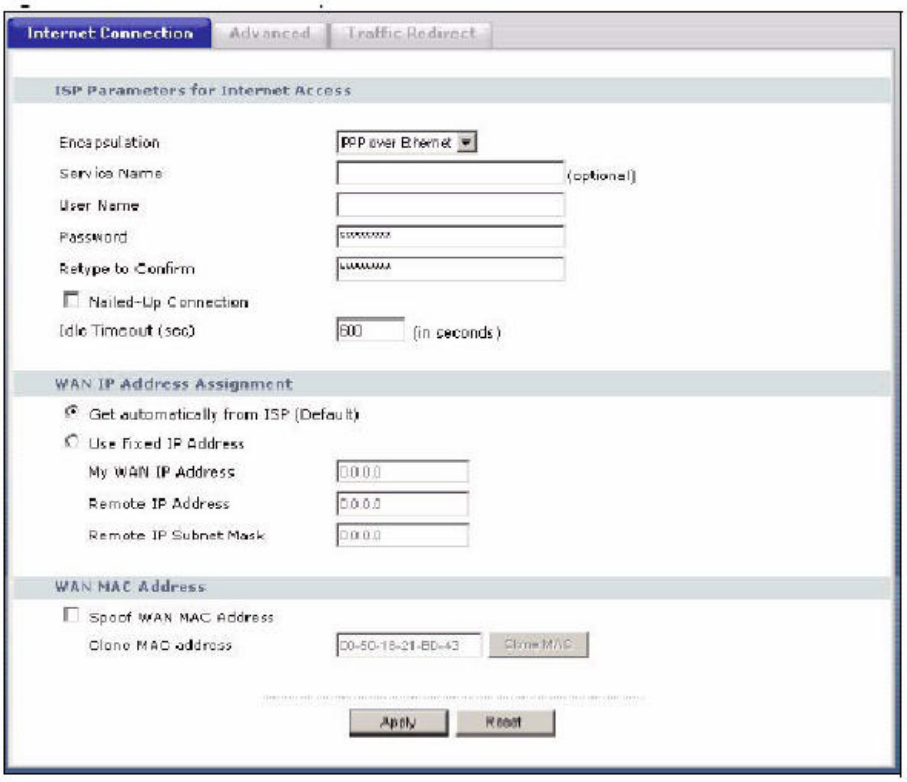
Uno de los beneficios del PPPoE es la habilidad para permitir el acceso a uno de los múltiples servicios de red, función conocida como selección dinámica del servicio. Esto permite al proveedor del servicio el crear y ofrecer de manera simple nuevos servicios IP para sus usuarios.

Operacionalmente, PPPoE supone un ahorro tanto para el lado cliente como para el ISP dado que no requiere una configuración específica compleja.

Mediante la implementación directa del PPPoE en el gateway, los ordenadores de la LAN no necesitan tener instalado ningún software PPPoE dado que el router realizará esa tarea. Asimismo, con el NAT, todos los ordenadores de la LAN dispondrán de acceso a Internet.

La siguiente pantalla muestra la encapsulación **PPPoE.**

Figura 45 WAN : Encapsulación PPPoE



La siguiente tabla describe las etiquetas de esta pantalla.

Tabla 32 WAN : Encapsulación PPPoE

ETIQUETA	DESCRIPCIÓN
Parámetros para el acceso a internet	
Encapsulación	La opción PPPoE es similar a una conexión telefónica a redes tradicional.
Nombre del servicio	Introduzca el nombre del servicio PPPoE que se le haya facilitado.
Nombre de usuario	Introduzca el nombre de usuario que se le haya facilitado.
Contraseña	Introduzca la contraseña asociada al nombre de usuario anterior.
Volver a teclear para confirmar	Vuelva a introducir la contraseña para asegurar que ha sido tecleada correctamente.
Conexión Forzada	Seleccione **Conexión forzada** si desea que la conexión esté siempre establecida.
Temporizador de inactividad	Este valor especifica el tiempo en segundos que pasarán sin que exista tráfico a través de esta sesión antes de que el router automáticamente la desconecte.
Asignación de Dirección IP WAN	
Obtener automáticamente del ISP	Seleccione esta opción si su ISP no le ha proporcionado una dirección IP fija.Ésta será la

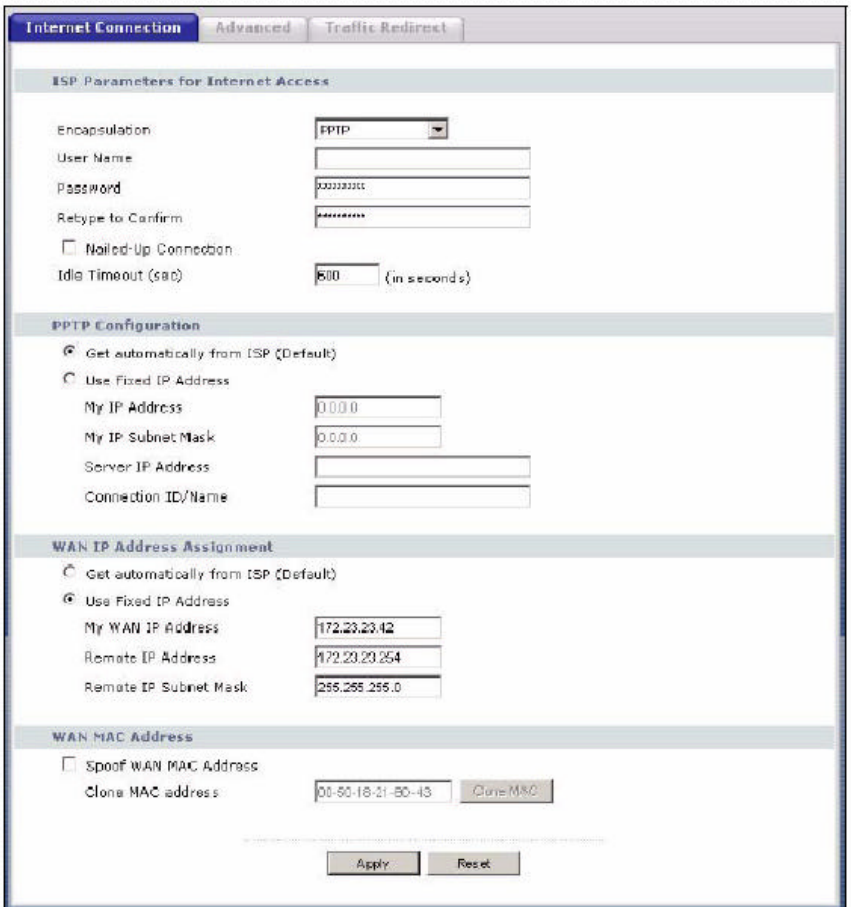
	opción por defecto.
Utilizar una dirección IP fija	Seleccione esta opción si su ISP le ha asignado una dirección IP fija.
Dirección IP	Introduzca la dirección IP WAN en este campo si ha seleccionado la opción Utilizar una dirección IP fija.
Máscara de subred	Introduzca la máscara de subred en este campo (si le ha sido facilitada por su ISP).
Puerta de enlace predeterminada	Introduzca la dirección de la puerta de enlace predeterminada (si le ha sido facilitada por su ISP)
Dirección MAC WAN	
Spoofing de la dirección MAC WAN	La sección de la dirección MAC permite a los usuarios el configurar la dirección MAC del puerto WAN bien utilizando la dirección por defecto o clonando la dirección MAC de un ordenador de LAN. No marcar la casilla de selección para utilizar la dirección MAC por defecto. Seleccionar esta opción y vaya sobre Clonar MAC para introducir la dirección MAC en el campo siguiente.
Clonar dirección MAC	Introducir la dirección MAC del ordenador de la LAN cuya MAC se va a clonar.
Aplicar	Pulse **Aplicar** para guardar los cambios.
Resetear	Pulse **Resetear** para volver a cargar en los parámetros de esta pantalla los valores previos.

5.6.3 Encapsulación PPTP

PPTP (Point-to-Point Tunneling Protocol) es un protocolo de red que posibilita la transferencia seguridad de datos desde un cliente remoto a un servidor privado, creando una VPN utilizando protocolos TCP/IP.

La pantalla siguiente muestra la configuración de una encapsulación **PPTP**.

Figura 46 Encapsulación PPTP



La siguiente tabla describe las etiquetas dentro de esta pantalla.

Tabla 33 Encapsulación PPTP

ETIQUETA	DESCRIPCIÓN
Parámetros para el acceso a internet	
Encapsulación	La opción PPTP es un protocolo de red que permite una transferencia de datos segura desde un cliente remoto a un servidor privado, creando una VPN utilizando protocolos TCP/IP. Para configurar un cliente PPTP, deberá configurar los campos del nombre de usuario y la contraseña para la conexión PPP y los parámetros PPTP para la conexión PPTP.
Nombre de usuario	Introduzca el nombre de usuario que se le haya facilitado.
Contraseña	Introduzca la contraseña asociada al nombre de usuario anterior.
Volver a teclear para confirmar	Vuelva a introducir la contraseña para asegurar que

	ha sido tecleada correctamente.
Conexión Forzada	Seleccione **Conexión forzada** si desea que la conexión esté siempre establecida.
Temporizador de inactividad	Este valor especifica el tiempo en segundos que pasarán sin que exista tráfico a través de esta sesión antes de que el router automáticamente la desconecte.
Configuración PPTP	
Obtener automáticamente del ISP	Seleccione esta opción si su ISP no le asigna una dirección IP fija. Ésta será la opción por defecto.
Utilizar una dirección IP fija	Seleccione esta opción si su ISP le asigna una dirección IP fija.
Mi dirección IP	Introduzca la dirección IP recibida de su ISP.
Mi máscara de subred	Su P320W automáticamente calculará la máscara de subred basada en la dirección IP asignada. A menos que se le indique lo contrario, utilice esta máscara de subred calculada por el router.
Dirección IP del servidor	Introduzca la dirección IP del servidor PPTP
Nombre /ID de la conexión	Introduzca el nombre de identificación para su servidor PPTP.
Asignación de Dirección IP WAN	
Obtener automáticamente del ISP	Seleccione esta opción si su ISP no le ha proporcionado una dirección IP fija.Ésta será la opción por defecto.
Utilizar una dirección IP fija	Seleccione esta opción si su ISP le ha asignado una dirección IP fija.
Dirección IP	Introduzca la dirección IP WAN en este campo si ha seleccionado la opción Utilizar una dirección IP fija.
Máscara de subred	Introduzca la máscara de subred en este campo (si le ha sido facilitada por su ISP).
Puerta de enlace predeterminada	Introduzca la dirección de la puerta de enlace predeterminada (si le ha sido facilitada por su ISP)
Dirección MAC WAN	
Spoofing de la dirección MAC WAN	La sección de la dirección MAC permite a los usuarios el configurar la dirección MAC del puerto WAN bien utilizando la dirección por defecto o clonando la dirección MAC de un ordenador de LAN. No marcar la casilla de selección para utilizar la dirección MAC por defecto. Seleccionar esta opción y vaya sobre Clonar MAC para introducir la dirección MAC en el campo siguiente.
Clonar dirección MAC	Introducir la dirección MAC del ordenador de la LAN cuya MAC se va a clonar.
Aplicar	Pulse **Aplicar** para guardar los cambios.
Resetear	Pulse **Resetear** para volver a cargar en los parámetros de esta pantalla los valores previos.

5.7 Pantalla de Opciones Avanzadas WAN

Para modificar las opciones avanzadas del interfaz WAN, pulse sobre **WAN** bajo las opciones **Red** y posteriormente en la pestaña **Avanzada**. Aparecerá la siguiente pantalla.

Figura 47 Opciones avanzadas

La siguiente tabla describe las etiquetas dentro de esta pantalla.

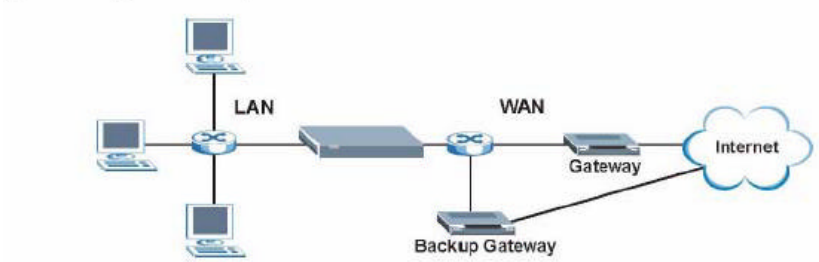
Tabla 34 Opciones avanzadas

ETIQUETA	DESCRIPCIÓN
Servidores DNS	
Servidor DNS Primario Servidor DNS Secundario	Introduzca las direcciones IP de los servidores DNS. Si no configura ningún servidor DNS, deberá conocer la dirección IP de las máquinas en internet para poder acceder a ellas.
Aplicar	Pulse **Aplicar** para guardar los cambios.
Resetear	Pulse **Resetear** para volver a configurar esta pantalla de nuevo.

5.8 Redirección de Tráfico

La redirección de tráfico encamina todo el tráfico WAN a través de una puerta de enlace de backup cuando el P320W no puede conectarse a Internet a través del gateway normal. Conecte el gateway de backup en la parte WAN, de manera que el P320W pueda seguir proporcionando protección mediante el firewall.

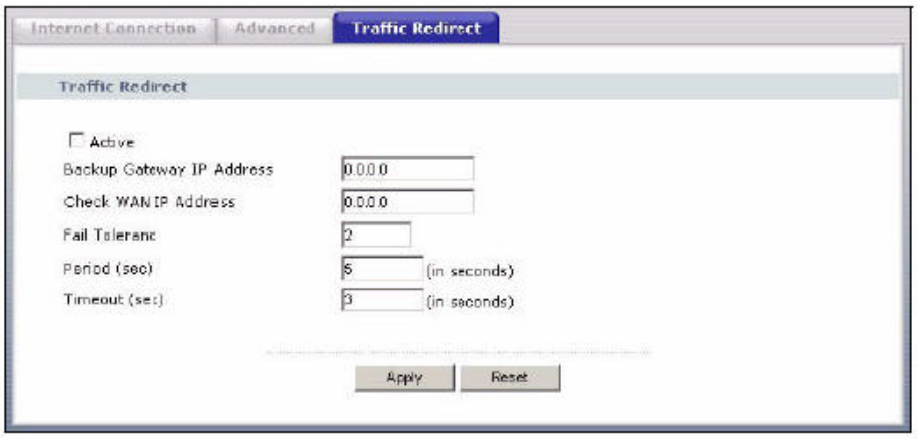
Figura 48 Configuración WAN para la redirección de tráfico



5.9 Pantalla de Redirección de Tráfico

Para modificar los parámetros de la Redirección de Tráfico en el P320W, pulse sobre el enlace WAN bajo las opciones de Red y acceda a la pestaña Redirección de Tráfico. Aparecerá la siguiente pantalla.

Figura 49 WAN: Redirección de Tráfico



La siguiente tabla describe las etiquetas de esta pantalla.

Tabla 35: Redirección de Tráfico

ETIQUETA	DESCRIPCIÓN
Activar	Seleccione esta casilla para que el P320W utilice la redirección de tráfico si la conexión WAN habitual falla.
Dirección IP del gateway de backup	Introduzca la dirección IP del gateway de backup.
Comprobación Dirección IP WAN	La configuración de este campo es opcional. Si no introduce ninguna dirección en este campo, el P320W utilizará la dirección IP de la puerta de enlace por defecto. Configure este campo para comprobar la accesibilidad de la WAN de su P320W. Introduzca la dirección IP de un equipo cercano fiable (por ejemplo, la dirección de un servidor DNS). Si está utilizando encapsulación PPTP ó PPPoE, introduzca "0.0.0.0" para configurar el P320W de manera que compruebe el estado del PVC o túnel PPTP.
Tolerencia	Introduzca el número de veces que el router deberá testear de forma fallida la conexión a internet a través de la interfaz WAN antes de reencaminar todo el tráfico por el gateway de backup.
Periodo (segundos)	Introduzca el número de segundos que el P320W esperará entre comprobaciones para verificar si es posible conectar con la dirección IP WAN (introducida en el campo **Comprobación Dirección IP WAN**) ó gateway por defecto. Permita un poco más de tiempo si la dirección IP destino debe manejar gran cantidad de tráfico.
Temporizador (segundos)	Introduzca el número de segundos que el P320W esperará a la respuesta del ping realizada a la dirección especificada en el campo **Comprobar Dirección IP WAN** antes de que expire. La conexión WAN se considera caída tras expirar esta prueba el número de veces configuradas en el campo Tolerancia. Utilice un valor elevado en este campo si la red está congestionada.
Aplicar	Pulse **Aplicar** para guardar los cambios.
Resetear	Pulse **Resetear** para volver a configurar la pantalla de nuevo.

CAPÍTULO 6: LAN

Este capítulo describe como configurar los parámetros de la LAN

6.1 Descripción LAN

La LAN (Local Area Network – Red de Área Local) es un sistema de comunicaciones compartido por múltiples ordenadores conectados. Las pantallas de LAN permiten configurar el servidor DHCP, la dirección IP de gestion así como dividir la red física en diferentes redes lógicas.

6.1.1 Configuración Pool IP

El P320W está preconfigurado con un pool de 32 direcciones IP comenzando en la 192.168.1.33 hasta la 192.168.1.64. Este configuración deja 31 direcciones IP (excluyendo la propia del P320W) en el rango inferior de manera que puedan ser utilizar por otros equipos servidores situados en la LAN, por ejemplo, servidores de correo, FTP, web,…. que puedan existir.

6.1.2 Servidores DNS

Consulte la sección *Dirección IP y Máscara de Subred* en el capítulo **Asistente de Conexión**.

6.2 LAN TCP/IP

El P320W implementa la funcionalidad de servidor DHCP que permite asignar direcciones IP y de servidores DNS a los equipos de la LAN que soportan la capacidad de cliente DHCP.

6.2.1 Parámetros por defecto de LAN

Los parámetros por defecto de la LAN del P320W se presentan con los siguientes valores:

• Dirección IP 192.168.1.1 con máscara de subred 255.255.255.0 (24 bits)

• Servidor DHCP habilitado con 32 direcciones IP de cliente comenzando por la 192.168.1.33.

Estos parámetros deberán funcionar en la mayoría de las instalaciones. Si su ISP le proporciona los datos con las direcciones de los servidores DNS, deberá introducir los mismos en los campos correspondientes.

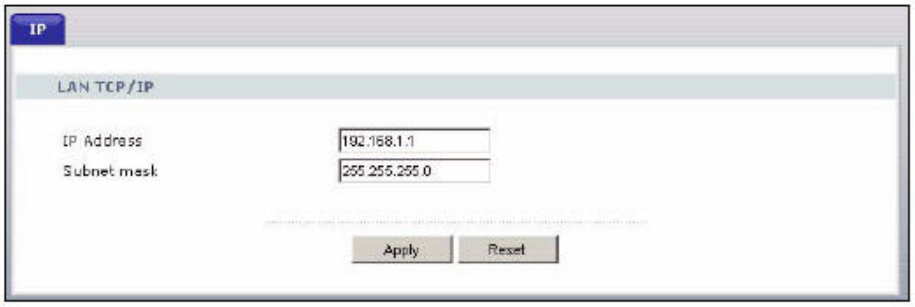
6.2.2 Dirección IP y Máscara de subred

Consulte la sección sobre la Dirección IP y la máscara de subred en el capítulo de **Asistente de Configuración**.

6.3 Pantalla IP

Pulse sobre el enlace **LAN** bajo las opciones de **Red** para abrir la pantalla **IP**.

Figura 50 LAN IP



La siguiente tabla describe las etiquetas de esta pantalla.

Tabla 36 LAN IP

ETIQUETA	DESCRIPCIÓN
TCP/IP LAN	
Dirección IP	Introduzca la dirección IP de su P320W (por defecto 192.168.1.1)
Máscara de subred	La máscara de subred especifica el número de red de una dirección IP. Su P320W calculará automáticamente la máscara de subred en base a la dirección IP tecleada.
Aplicar	Pulse **Aplicar** para guardar los cambios.
Resetear	Pulse **Resetear** para volver a configurar esta pantalla de nuevo.

CAPÍTULO 7: SERVIDOR DHCP

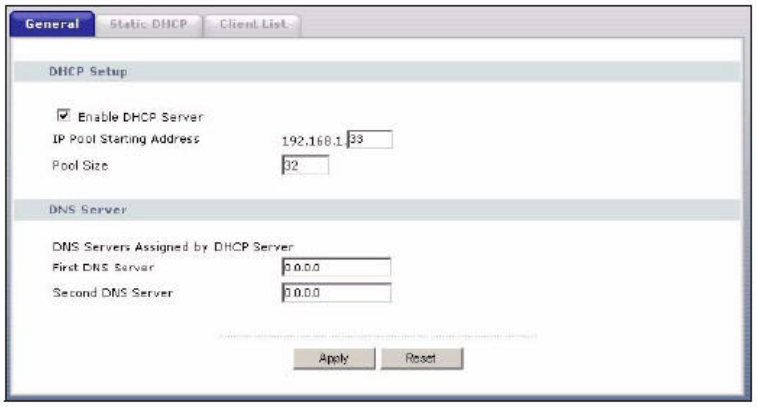
7.1 DHCP

El protocolo DHCP (Dynamic Host Configuration Protocol) permite a clientes individuales el obtener la configuración TCP/IP al iniciarse, desde un servidor. Es posible configurar el P320W como servidor DHCP o simplemente deshabilitarlo. Cuando se configura como servidor, el P320W proporciona la configuración TCP/IP a los clientes. Si el servidor DHCP está deshabilitado, será necesario disponer de algún otro servidor DHCP en LAN o bien configurar de forma manual los parámetros en cada ordenador.

7.2 Pantalla DHCP

Pulse sobre el enlace Servidor DHCP bajo las opciones Red y seleccione la pestaña General. Se le mostrará la siguiente pantalla.

Figura 51 General



La siguiente tabla describe las etiquetas de esta pantalla.

Tabla 37 General

ETIQUETA	DESCRIPCIÓN
Habilitar Servidor DHCP	Deje esta casilla sin marcar para deshabilitar el servidor DHCP del P320W. Cuando se configure como servidor, el router proporcionará los parámetros TCP/IP a los clientes de la LAN que lo soliciten. Si no, con el servidor DHCP deshabilitado será necesario disponer de algún otro servidor DHCP en LAN o configurar los parámetros TCP/IP de forma manual en cada cliente. Cuando actúe como servidor, complete los siguientes campos.
Dirección IP Comienzo del Pool	Este campo especifica la primera de las direcciones IP del pool.
Tamaño del Pool	Esta campo especifica el tamaño del pool de direcciones.
Servidores DNS asignados por el Servidor DHCP El P320W transfiere la dirección IP de los servidores DNS (Domain Name System) a los clientes DHCP. El gateway únicamente pasará la información a los clientes DHCP en la LAN cuando se marque la casilla Habilitar Servidor DHCP. Cuando esta casilla no se marque, el servicio DHCP quedará deshabilitado y deberá disponer de otro servidor DHCP en LAN o configurar las direcciones de los servidores DNS manualmente en cada ordenador.	
Servidor DNS Primario Servidor DNS Secundario	Introduzca las direcciones IP de los servidores DNS. Si no configura ningún servidor DNS, necesitará conocer la dirección IP de las máquinas a las que desee acceder.
Aplicar	Pulse **Aplicar** para guardar los cambios.
Resetear	Pulse **Resetear** para volver a configurar esta pantalla de nuevo.

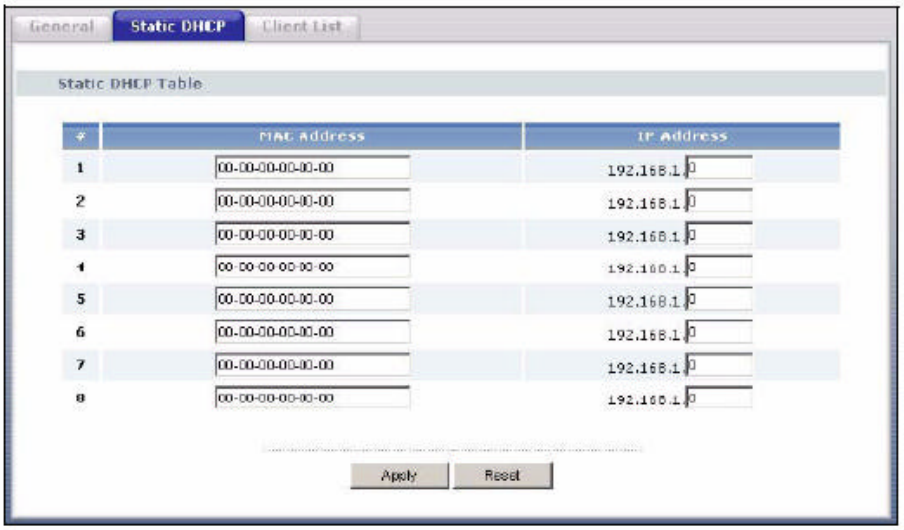
7.3 Pantalla DHCP Estático

Esta tabla permite asignar direcciones IP a determinados equipos ubicados en la LAN en función de sus direcciones MAC.

Cada dispositivo Ethernet dispone de una dirección MAC (Media Access Control) única. La dirección MAC es asignada en la fabricación y consiste en seis pares de caracteres hexadecimales, por ejemplo, 00:A0:C5:00:00:02.

Para modificar los parámetros del DHCP Estático del P320W, pulse sobre el enlace **Servidor DHCP** bajo las opciones de **Red** y vaya a la pestaña **DHCP Estático**. Se mostrará la siguiente pantalla.

Figura 52 DHCP Estático



La siguiente tabla describe las etiquetas de esta pantalla.

Tabla 38 DHCP Estático

ETIQUETA	DESCRIPCIÓN
#	Este campo es el índice de la entrada en la tabla
Dirección MAC	Introduzca la dirección MAC de un ordenador de su LAN
Dirección IP	Introduzca la dirección IP que se deberá asignar al ordenador de su LAN
Aplicar	Pulse **Aplicar** para guardar los cambios
Resetear	Pulse **Resetear** para volver a configurar esta pantalla de nuevo.

7.4 Pantalla Lista de Clientes

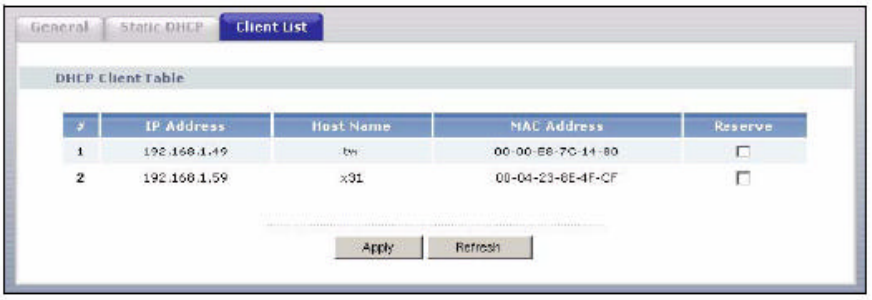
La tabla DHCP muestra la información sobre los clientes DHCP (incluyendo dirección IP, Nombre del Host y Dirección MAC) actualmente utilizando el servidor DHCP del P320W.

Para visualizar esta pantalla pulse sobre el enlace **Servidor DHCP** bajo las opciones **Red** y a continuación seleccione la pestaña **Lista de Clientes**.

Nota: También puede visualizar la lista de clientes de sólo-lectura pulsando sobre el enlace **Tabla DHCP(Detalles)** en la pantalla **Status (Estado).**

Se mostrará la siguiente pantalla.

Figura 53 Lista de Clientes



La siguiente tabla describe las etiquetas de esta pantalla.

Tabla 39 Lista de Clientes

ETIQUETA	DESCRIPCIÓN
#	Este campo es el índice para el ordenador dentro de la lista
Dirección IP	Este campo muestra la dirección IP relativa a la entrada # indicada anteriormente.
Nombre de Host	Este campo muestra el nombre del ordenador.
Dirección MAC	Este campo muestra la dirección MAC del adaptador de red utilizado por el ordenador para conectarse con el P320W.
Reservado	Seleccione esta casilla para que el P320W siempre asigne la dirección IP actual a esa dirección MAC (y nombre de equipo). Puede seleccionar hasta 8 entradas en esta tabla. Tras pulsar sobre **Aplicar**, la dirección MAC y la dirección IP también aparecerán en la pantalla DHCP Estático.
Aplicar	Pulse **Aplicar** para guardar los cambios
Refrescar	Pulse **Refrescar** para volver a cargar la información de la tabla DHCP.

CAPÍTULO 8: NAT

Este capítulo describe como configurar la funcionalidad NAT en el gateway

8.1 Descripción NAT

La funcionalidad NAT (Network Address Translation) consiste en la traslación de la dirección IP del equipo dentro del paquete. Por ejemplo, la dirección origen de un paquete saliente, utilizado dentro de una red será modificado por una dirección IP diferente conocida dentro de otra red.

8.1.1 Definiciones NAT

Los términos “interno” y “externo” nos indican donde se encuentra localizado un host con respecto al P320W. Por ejemplo, los ordenadores de los clientes son los equipos internos mientras que los servidores Web en Internet son los equipos externos.

Los términos “global” y “local” indican la dirección IP de un host en el paquete que atraviesa el router. Por ejemplo, la dirección local se refiere a la dirección IP de un host cuando el paquete se encuentra en la red local, mientras que la dirección global se refiere a la dirección IP del host cuando el mismo paquete pasa a través del lado WAN.

Tener en consideración que interno/externo hace referencia a la localización del host, mientras que global/local hace referencia a la dirección IP del host utilizada en un paquete. De manera que, una dirección local interna (ILA) es la dirección IP de un host interno en un paquete cuando el mismo se encuentra todavía en la red local, mientras que una dirección global interna (IGA) es la dirección IP del mismo host interno cuando el paquete se encuentra en el lado WAN.

La siguiente tabla resume esta información.

Tabla 40 Definiciones NAT

TÉRMINO	DESCRIPCIÓN
Interno	Hace referencia a un host en el lado LAN
Externo	Hace referencia a un host en el lado WAN
Local	Hace referencia a la dirección del paquete (origen o destino) cuando el paquete viaja en la LAN.
Global	Hace referencia a la dirección del paquete (origen o destino) cuando el paquete viaja a través de la WAN.

Nota: El NAT nunca modifica la dirección IP (local o global) de un host externo.

8.1.2 Qué hace el NAT

De forma más simple, el NAT cambia la dirección IP origen de un paquete recibido de un usuario (dirección local interna) en otra (dirección global interna) antes de enviar el paquete hacia el lado WAN. Cuando la respuesta vuelve, el NAT traslada la dirección destino (dirección global interna) a la dirección local interna antes de enviarlo hacia el host que originó la petición. Hacer ver como la dirección IP (bien local o global) de un host externo nunca es modificada.

Las direcciones IP globales para los hosts internos pueden ser bien estáticas o dinámicas asignadas por el ISP.

Adicionalmente, es posible colocar servidores (por ejemplo servidor Web o telnet) en el lado de red local y hacerlo accesible al mundo externo. Si no define ningún servidor el NAT ofrece el beneficio adicional de la protección de un firewall. Cuando no se definen servidores, el P320W filtra todas las peticiones entrantes, lo que previene que posible intrusiones penetren en la red local.

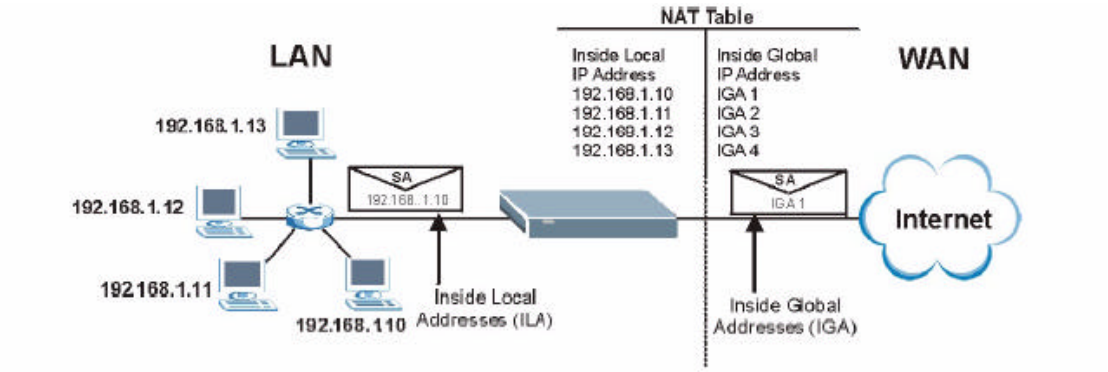
8.1.3 Cómo funciona el NAT

Cada paquete tiene dos direcciones – una dirección origen y una dirección destino. Para los paquetes salientes, la ILA (Inside Local Address) es la dirección origen en la LAN, y la IGA (Inside Global Address) es la dirección origen en la WAN. Para los paquetes entrantes, la ILA es la dirección destino en la LAN y la IGA es la dirección destino en la WAN.

El NAT mapea las direcciones IP privadas (locales) a las únicas direcciones globales requeridas para la comunicación con hosts en otras redes. De manera que reemplaza la dirección IP origen en cada paquete y después lo envía hacia Internet.

El P320W mantiene un rastro de las direcciones origen y el número de puerto de manera que los paquetes respuesta puedan ver restaurados sus valores originales. La siguiente figura ilustra esta explicación.

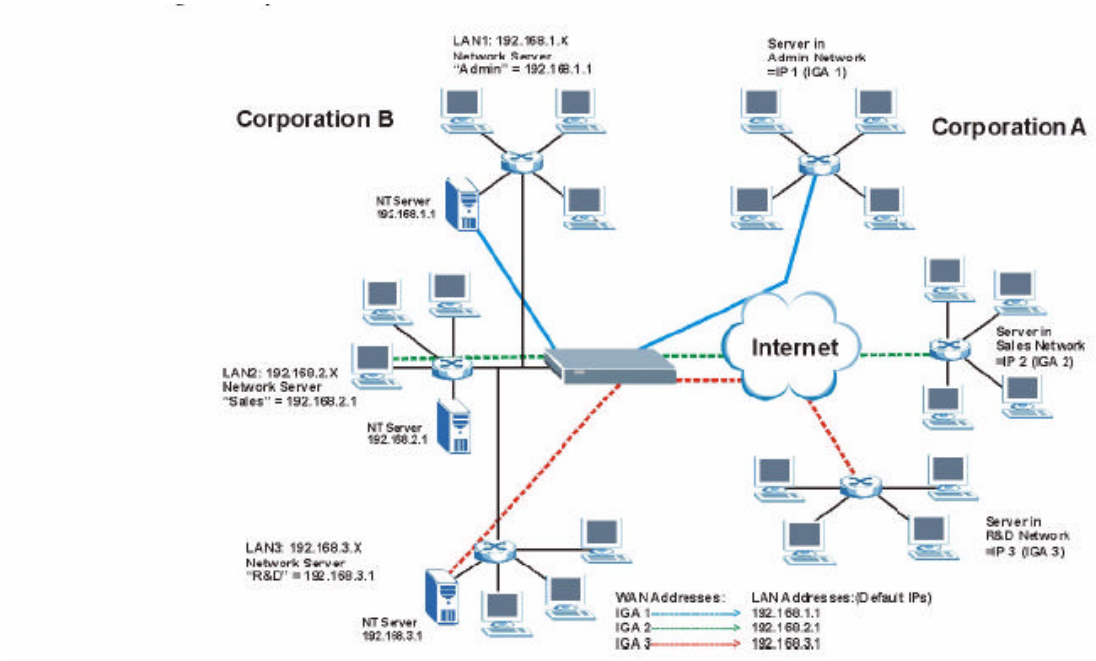
Figura 54 Cómo funciona el NAT



8.1.4 Aplicaciones NAT

La siguiente figura ilustra una posible aplicación NAT, donde tres LANs internas (redes lógicas utilizando IP Alias) tras el P320W pueden comunicarse con tres redes WAN diferentes. Al final de este capítulo se explican ejemplos adicionales.

Figura 55 Aplicación NAT con IP Alias



8.1.5 Dirección IP de la Estación por defecto

Adicionalmente a los servidores para servicios específicos, el NAT soporta la dirección IP de un servidor por defecto. Un servidor por defecto recibe los paquetes destinados a los puertos que no se especifican en esta pantalla.

Nota: Si no asigna ningún valor a la Dirección IP de la Estación por defecto, el P320W descarta todos los paquetes recibidos por los puertos que no se encuentran especificados en esta pantalla o en la de gestión remota.

8.1.6 Reenvío de puertos: Servicios y Números de Puerto

El conjunto de servidores SUA es una lista de servidores internos (tras el NAT en la LAN), por ejemplo, Web o FTP, que pueden estar accesibles al mundo exterior incluso cuando el NAT hace que toda su red interna aparezca como una única máquina hacia el exterior.

Utilice la pantalla de Reenvío de puertos para reenviar las peticiones de servicio recibidas por el P320W hacia el servidor ubicado en la red local. Será necesario teclear el número de puerto individual o rango de puertos a ser reenviados, y la dirección IP local del servidor deseado. El número de puerto identifica un servicio; por ejemplo, el servicio Web utiliza el puerto 80 y FTP el puerto 21. En algunos casos, tales como para servicios desconocidos o donde un servidor puede soportar más de un servicio (por ejemplo soportando tanto el servicio Web como FTP), lo más recomendable sería especificar un rango de puertos.

Adicionalmente a los servidores para servicios específicos, el NAT soporta un servidor por defecto. Una petición de servicio que no corresponda con un servidor explícitamente configurado, será reenviada al servidor por defecto. Si el servidor por defecto no está definido, la petición de servicio es simplemente descartada.

Los números de puertos más utilizados se muestran en la siguiente tabla. Consulte la RFC 1700 para más información sobre los números de puerto.

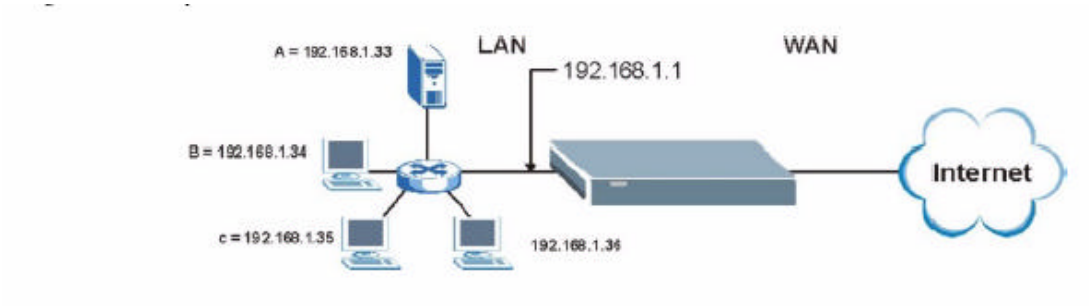
Tabla 41 Servicios y Números de puerto

SERVICIO	NÚMERO DE PUERTO
ECHO	7
FTP (File Transfer Protocol)	21
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer Protocol o WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161
SNMP trap	162
PPTP (Point-to-Point Tunneling Protocol)	1723

8.1.7 Configuración de Servidores tras el SUA (Ejemplo)

Supongamos que se desean asignar los puertos 21-25 a un servidor FTP, Telnet y SMTP (A en el ejemplo), puerto 80 para otro (B en el ejemplo) y asignar el servidor por defecto a la dirección IP 192.168.1.35 de un tercero (C en el ejemplo). El usuario asigna la dirección IP de LAN y el ISP asigna la dirección IP de WAN. El NAT hace que la red local aparezca como un host único en Internet.

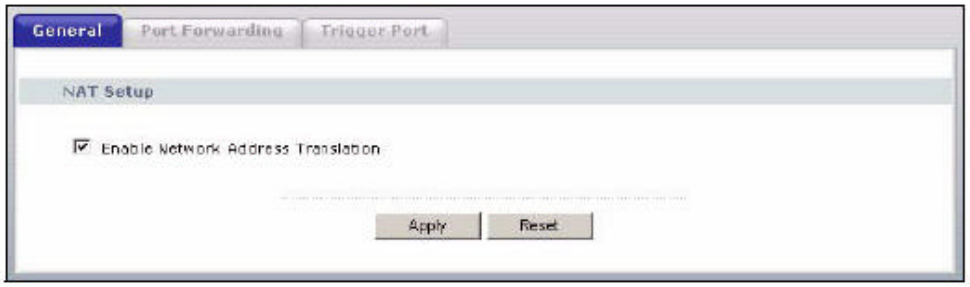
Figura 56 Múltiples servidores tras el NAT



8.2 Pantalla NAT General

Pulse sobre el enlace **NAT** bajo las opciones **Red** para abrir la pantalla **General**.

Figura 57 NAT : General



La siguiente tabla describe las etiquetas de esta pantalla.

Tabla 42 NAT : General

ETIQUETA	DESCRIPCIÓN
Habilitar la Traslación de Direcciones de Red	El NAT permite la traslación de una dirección interna utilizada en una red en una dirección IP diferente conocida dentro de otra red. Seleccione la casilla para habilitar el NAT.
Aplicar	Pulse **Aplicar** para guardar los cambios.
Resetear	Pulse **Resetear** para configurar de nuevo los parámetros de esta pantalla.

8.3 Pantalla del Reenvío de Puertos

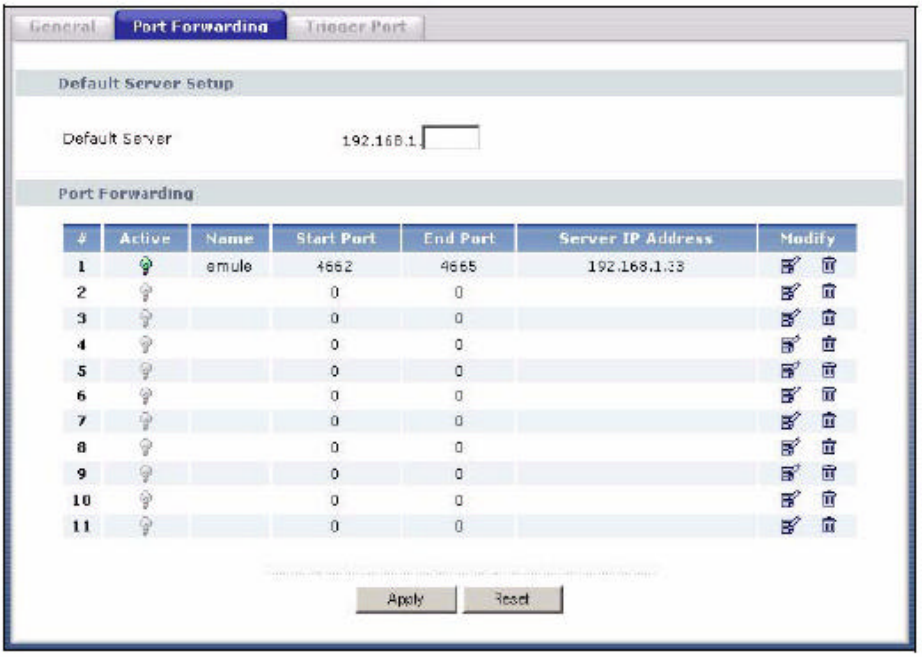
El orden de las reglas es importante dado que el P320W aplica las reglas de forma ordenada según se especifican. Cuando un paquete coincide con una regla, el P320W realiza la acción correspondiente y las reglas pendientes son ignoradas. Si existen reglas vacías delante de alguna nueva regla, ésta será adelantada el número de reglas vacías existentes. Por ejemplo, si se han configurado de las reglas 1 a la 6 y ahora se configura la regla 9. En la pantalla resumen, la nueva regla será colocada como regla 7, no 9. Ahora si se borra la regla 4, de las reglas 5 a la 7 serán colocadas ahora entre la 4 y la 6.

Consulte la Tabla 41 para más información sobre los números de puerto comúnmente utilizados por servicios particulares.

Nota: Si no asigna ninguna dirección IP al Servidor por defecto, el P320W descartará todos los paquetes recibidos a puertos no especificados en este pantalla o en la gestión remota.

Para modificar los parámetros del Reenvío de puertos del P320W, pulse sobre el enlace **NAT** bajo las opciones **Red** y seleccione la pestaña **Reenvío de puertos**. La pantalla que aparecerá será como la siguiente.

Figura 58 Reenvío de puertos



La siguiente tabla describe las etiquetas de esta pantalla.

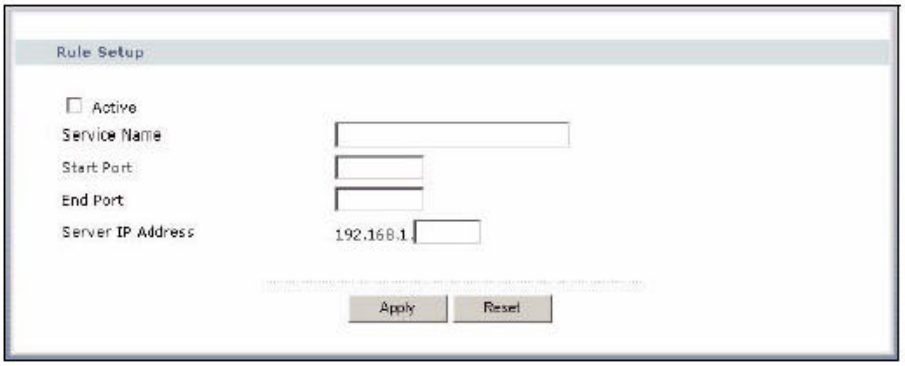
Tabla 43 NAT : Reenvío de puertos

ETIQUETA	DESCRIPCIÓN
Servidor por defecto	Adicionalmente a los servidores para servicios específicos, el NAT soporta la definición de un servidor por defecto. Un servidor por defecto reciba todos los paquetes dirigidos a todos los puertos que no se especifican en esta pantalla.
#	Número de una entrada individual NAT.
Activo	Este icono está encendido cuando la entrada está habilitada. Pulse sobre el icono de edicción bajo **Modificar** y seleccione la casilla **Activar** en la pantalla de **Configuración de Regla** para habilitar la entrada del reenvío de puerto. Desmarque la casilla para deshabilitar el reenvío de estos puertos al servidor interno sin tener que borrar la entrada.
Nombre	Este campo muestra el nombre para identificar a esta regla de reenvío.
Puerto inicial	Este campo muestra el número de puerto inicial
Puerto final	Este campo muestra el número de puerto final. Si el número de puerto es el mismo que el del campo **Puerto inicial**, únicamente un puerto individual será reenviado. Si se coloca un puerto diferente que el mostrado en el campo anterior, el reenvío se hará sobre un rango de puertos.
Dirección IP Servidor	Este campo muestra la dirección IP del servidor interno.
Modificar	Pulse sobre el icono de edicción para abrir la pantalla de la regla creada. Modificar una regla existente o crear una nueva regla en la pantalla **Configuración de Reglas**.
Aplicar	Pulse **Aplicar** para guardar los cambios
Resetear	Pulse **Resetear** para volver a configurar los parámetros de esta pantalla de nuevo.

8.3.1 Pantalla de Configuración de Reglas

Para editar una regla de reenvío, pulse sobre el icono de edición bajo **Modificar**. Aparecerá la siguiente pantalla.

Figura 59 NAT :Reenvío de puertos : Configuración de Reglas



La siguiente tabla describe las etiquetas dentro de esta pantalla.

Tabla 44 NAT : Reenvío de puertos : Configuración de reglas

ETIQUETA	DESCRIPCIÓN
Activo	Seleccione esta casilla para habilitar esta entrada. Desmarcar la casilla para deshabilitar el reenvío sin necesidad de eliminar la entrada.
Nombre del servicio	Introduzca el **Nombre del servicio** para identificar esta regla.
Puerto inicial	Introduzca el número de puerto inicial. Para reenviar un único puerto, introduzca nuevamente en el siguiente campo el mismo número. Para especificar rangos, introduzca el puerto final a ser reenviado en el campo **Puerto final**.
Puerto final	Introduzca el número de puerto final.
Dirección IP Servidor	Introduzca la dirección IP interna del servidor
Aplicar	Pulse **Aplicar** para guardar los cambios.
Cancelar	Pulse **Cancelar** para volver a la pantalla previa sin guardar los cambios.

8.4 Triggering de Puertos

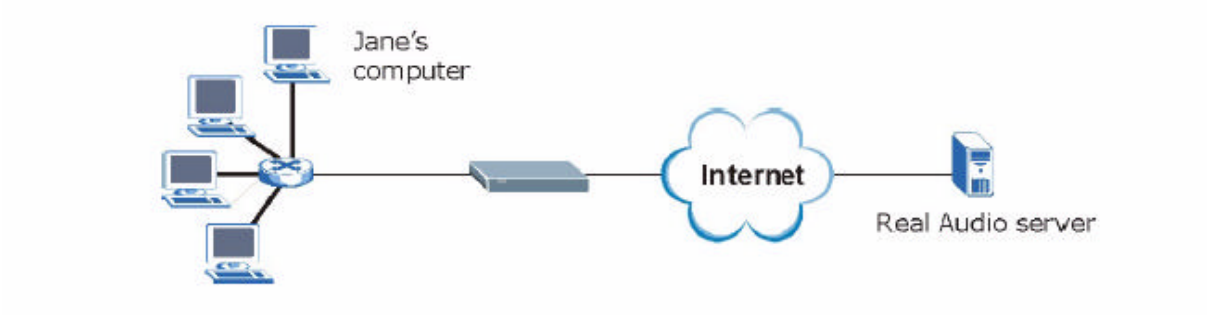
Algunos servicios utilizan un rango de puertos dedicado en el lado cliente y un rango de puertos dedicado en el lado servidor. Con el reenvío de puertos tradicional se configura dicho reenvío en el NAT para que el servicio recibido (desde un servidor en WAN) sea expedido a una dirección IP de un ordenador en el lado cliente (LAN). El problema es que el reenvío de puertos únicamente permite el disfrutar del servicio a una dirección IP única de la LAN. Para utilizar el mismo servicio en un ordenador diferente de la LAN, será necesario reemplazar de forma manual la dirección IP de la LAN en el reenvío de puertos.

El triggering de puertos solventa este problema permitiendo que diferentes ordenadores en la LAN puedan dinámicamente utilizar este servicio por turnos. El P320W mantiene un registro con la dirección IP del ordenador de la LAN que envía hacia la WAN solicitando un servicio con un número de puerto específico y protocolo (puerto de “lanzamiento”). Cuando el puerto WAN del P320W recibe la respuesta con un número de puerto específico y protocolo (puerto “entrante”), el P320W envía todo el tráfico a la dirección IP de LAN que envió la petición. Cuando finaliza la conexión del ordenador con el servicio, otro ordenador en la LAN puede utilizar el servicio de la misma manera. Este mecanismo no necesita configurar una nueva dirección IP cada vez que se desea que un ordenador diferente de la LAN utilice la aplicación.

8.4.1 Ejemplo de Triggering de puertos

A continuación se muestra un ejemplo de triggering (lanzamiento) de puertos.

Figura 60 Proceso de triggering de puertos



1. Jane solicita un fichero del servidor Real Audio (puerto 7070).
2. El puerto 7070 es el puerto “trigger” que realiza el lanzamiento y origina que el P320W mantenga el registro de la dirección IP del ordenador de Jane. El P320W asocia la dirección IP del ordenador de Jane con el rango de puertos “entrantes” entre 6970-7170.
3. El servidor Real Audio responde utilizando un número de puerto entre 6970-7170.
4. El P320W reenvía el tráfico a la dirección IP del ordenador de Jane.
5. Únicamente Jane puede conectar con el servidor Real Audio hasta que la conexión se cierre o expire la conexión. El P320W tiene un temporizador de tres minutos con UDP (User Datagram Protocol), o dos horas con TCP/IP (Transfer Control Protocol/Internet Protocol).

8.4.2 Dos puntos a recordar sobre el Triggering de puertos

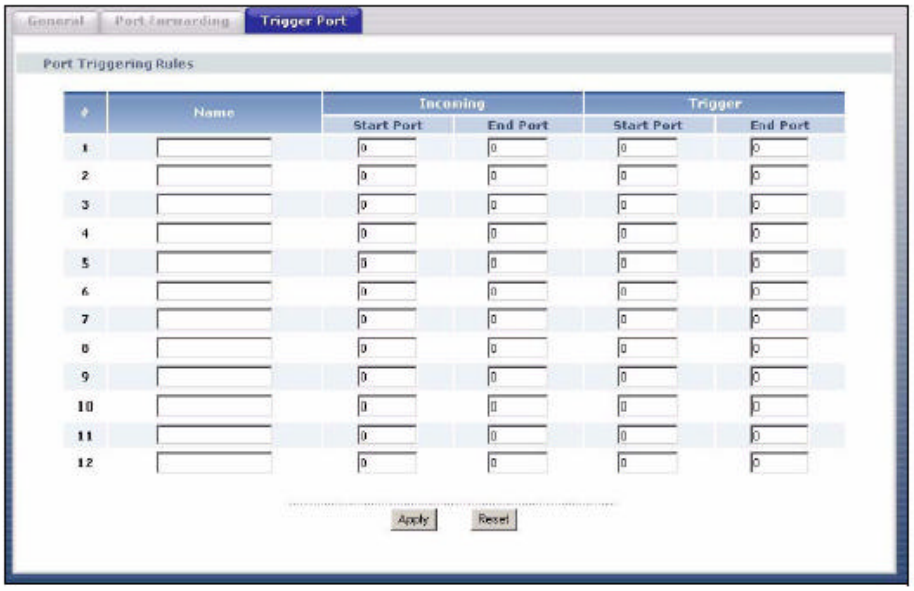
1. Los eventos trigger únicamente tienen lugar en los datos que van desde la red interna del P320W hacia el exterior.
2. Si una aplicación necesita un stream continuo de datos, el puerto (rango) será reservado de manera que ningún otro ordenador de la LAN podrá hacer uso de los mismos.

8.5 Pantalla del Triggering de puertos

Para modificar los parámetros del triggering de puertos, pulse sobre NAT bajo las opciones Red y seleccione la pestaña Lanzamiento de puertos. Aparecerá una pantalla como la siguiente.

Nota: Únicamente un ordenador en la LAN podrá utilizar un puerto trigger (de lanzamiento) a la vez.

Figura 61 NAT : Triggering de puertos



La siguiente tabla describe las etiquetas dentro de esta pantalla.

Tabla 45 NAT : Triggering de puertos

ETIQUETA	DESCRIPCIÓN
#	Este campo es el número del índice de la regla (sólo-lectura)
Nombre	Introduzca un nombre (de hasta 15 caracteres) con propósitos identificativos.
Entrada	Este campo identifica el puerto (o rango de puertos) que utiliza un servidor en WAN cuando envía un determinado servicio. El P320W envío el tráfico con este puerto (o rango de puertos) al cliente de la LAN que lo haya requerido.
Puerto inicial	Introduzca el número de puerto o puerto inicial del rango de puertos
Puerto final	Introduzca el número de puerto o puerto final del rango de puertos
Trigger	Este campo identifica el puerto (o rango de puertos) que origina (o lanza) al P320W a registrar la dirección IP del ordenador de la LAN que envía tráfico hacia un servidor en internet.
Puerto inicial	Introduzca el número de puerto o puerto inicial del rango de puertos
Puerto final	Introduzca el número de puerto o puerto final del rango de puertos
Aplicar	Pulse **Aplicar** para guardar los cambios
Resetear	Pulse **Resetear** para volver a configurar esta pantalla de nuevo.

CAPÍTULO 9: FIREWALL

Este capítulo describe alguna información general sobre firewalls y explica como configurar el fire wall implementado en este P320W

9.1 Introducción al Firewall

9.1.1 ¿Qué es un firewall?

Originalmente, el término firewall iba referido a la técnica de construcción diseñada para prevenir la propagación de un fuego desde una habitación a otra. El término de red "firewall" es un sistema o grupo de sistemas que fuerza una política de control de acceso entre dos redes. También debe definirse un mecanismo utilizado para proteger una red segura de una red no segura. Por supuesto, los firewalls no pueden resolver todos los problemas de seguridad. Un firewall es un mecanismo de seguridad utilizado para establecer un perímetro de seguridad en red basado en políticas de seguridad.

Nunca debería basarse en un único mecanismo o método de protección. Para que un firewall sea efectivo, se deberá diseñar de forma adecuada, esto requiere la integración del firewall en una política de seguridad amplia. Adicionalmente, las políticas específicas deberán ser implementadas dentro del mismo firewall.

9.1.2 Firewall de Inspección de Estado

Los firewalls basados en la inspección de estado restringuen el acceso comprobando los paquetes de datos frente a reglas de acceso definidas. Éstas llevan a cabo decisiones de control de acceso basándose en la dirección IP y protocolo.

Igualmente "inspeccionan" la sesión de datos para asegurar la integridad de la conexión y la adaptación a protocolos dinámicos. Estos firewalls generalmente proporcionan la mejor velocidad y transparencia, sin embargo, echan en falta la granularidad del control de acceso del nivel de aplicación.

Los firewalls, de uno u otro tipo, se han convertido en una parte integral del estándar de soluciones para seguridad en las empresas.

9.1.3 Sobre el Firewall del P320W

El firewall del Prestige es un firewall stateful inspection y está diseñado para proteger frente a ataques Denial of Services (Denegación de Servicio) cuando el mismo está activo (seleccione la pestaña **General** bajo **Firewall** y a continuación pulse sobre la casilla **Habilitar Firewall**). El propósito del Prestige es permitir a una red privada local (LAN) conectarse de forma segura a internet. El Prestige puede ser utilizado para prevenir el hurto, destrucción o modificación de datos, así como registrar estos eventos, lo cuál puede ser importante para la seguridad de su red. El Prestige también incorpora funcionalidades de filtrado de paquetes.

El Prestige es instalado entre la LAN y una conexión de acceso de banda ancha. Esto le permite actuar como un gateway seguro para todos los datos que pasan entre Internet y la LAN.

El Prestige cuenta con un puerto WAN y cuatro puertos Ethernet LAN, que son utilizados para separar físicamente la red en dos zonas. Donde el puerto WAN se utiliza para conectarse a la conexión externa mientras que el puerto de LAN se utiliza para conectar la red de ordenadores internos, los cuáles necesitan protegerse del mundo exterior.

9.1.4 Consejos para mejorar la seguridad con su Firewall

1. Cambie la contraseña por defecto del configurador web.
2. Limite el número de personas que podrán acceder a gestionar el router.
3. No habilite ningún servicio local (tales como SNMP o NTP) que no vaya a utilizar. Cualquier servicio habilitado puede presentar un riesgo potencial de seguridad. Cualquier hacker podría ser capaz de encontrar algún camino para acceder a través de estos servicios habilitados al firewall o a la red.
4. Para los servicios locales habilitados, protéjalos frente a un uso erróneo. Configúrelos para comunicarse únicamente con pares específicos, y asegúrelos configurando reglas para bloquear paquetes para los servicios en interfaces específicos.
5. Protéjase frente al IP Spoofing verificando que el firewall está activado.
6. Mantenga el firewall en una sala segura.

9.2 Pantalla General del Firewall

Pulse sobre el enlace **Firewall** bajo las opciones **Seguridad** para abrir la pantalla **General**.

Figura 62 Firewall : General

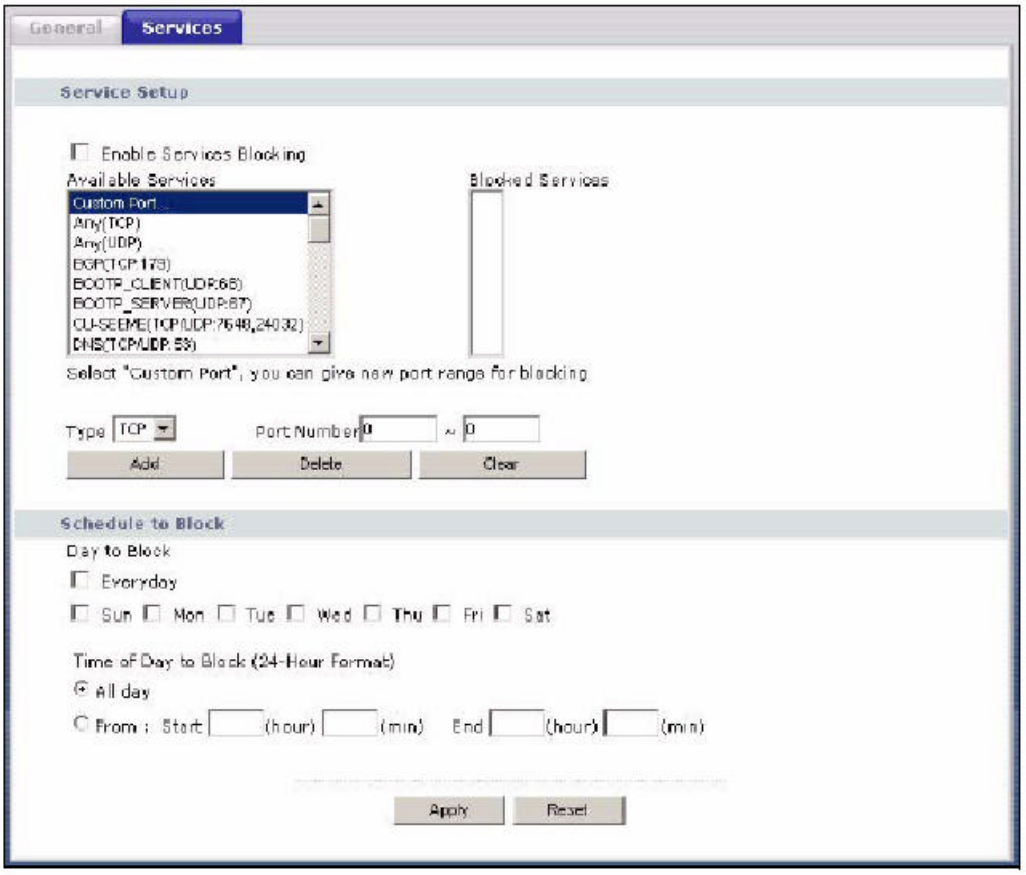
La siguiente tabla describe las etiquetas de esta pantalla.

ETIQUETA	DESCRIPCIÓN
Habilitar firewall	Seleccione esta casilla para activar el firewall. El P320W realiza un control de acceso y protege frente a ataques DoS (Denial of Service) cuando el firewall está activado.
Aplicar	Pulse **Aplicar** para guardar los cambios.
Resetear	Pulse **Resetear** para volver a configuración esta pantalla de nuevo.

9.3 Pantalla Servicios

Pulse sobre el enlace Firewall bajo las opciones de Seguridad y seleccione la pestaña Servicios. La pantalla que aparecerá será como la que se muestra a continuación. Utilice esta pantalla para habilitar el bloqueo de servicios, introducir/borrar/modificar servicios que se desean bloquear así como la fecha/hora en la que se desea se lleven a cabo esos bloqueos.

Figura 63 Firewall : Servicios



La siguiente tabla describe las etiquetas de esta pantalla.

Tabla 47 Firewall : Servicios

ETIQUETA	DESCRIPCIÓN
Habilitar Bloqueo de Servicios	Seleccione esta casilla para habilitar esta funcionalidad.
Servicios Disponibles	Aquí se muestra la lista de servicios pre-definidos (puertos) que pueden ser prohibidos a los usuarios de la LAN. Consulte la sección 9.3.1 para más información sobre estos servicios disponibles. Seleccione el puerto que desea bloquear de la lista desplegable y pulse **Añadir** para incluir el puerto en el campo de **Servicios Bloqueados**.
Servicios Bloqueados	Aquí se muestra la lista de servicios que no serán accesibles a los usuarios situados en la LAN una vez se habilite el bloqueo. Escoja el puerto (TCP, UDP ó TCP/UDP) que definan el puerto personalizado de la lista desplegable.
Puerto personalizado	Un puerto personalizado es un servicio que no se encuentra disponible en la lista de Servicios pre-definidos, el cuál será necesario definirlo utilizando los siguientes dos campos.
Tipo	Los servicios pueden ser TCP y/o UDP. Seleccione entre TCP o UDP.
Número de Puerto	Introduzca el rango de puertos que definen al servicio.
Añadir	Seleccione un servico de la lista de **Servicios Disponibles** y pulse **Añadir** para incluirlo en la lista de **Servicios Bloqueados**.
Eliminar	Seleccione un servicio de la lista de **Servicios Bloqueados** y pulse sobre **Eliminar** para quitarlo de la lista.
Limpiar	Pulse **Limpiar** para borrar la lista de **Servicios Bloqueados.**

Días de Bloqueo:	Seleccione la casilla correspondiente para configurar los días de la semana (o todos los días) en los que se desee activar este filtrado de contenidos.
Hora del día a bloquear (formato 24-horas)	Seleccione la hora del día en la que desee que el bloqueo tenga efecto.
Aplicar	Pulse **Aplicar** para guardar los cambios.
Resetear	Pulse **Resetear** para volver a configurar todos los parámetros de la pantalla de nuevo.

9.3.1 Servicios

Los servicios y los números de puerto utilizados más frecuentemente se muestran en la siguiente tabla. Por favor, consulte la RFC1700 para obtener más información. Junto con el nombre del servicio, aparecen dos campos entre corchetes. El primer campo indica el tipo de protocolo IP (TCP, UDP o ICMP). El segundo campo indica el número de puerto IP que define al servicio.

Tabla 48 Servicios más comunes

SERVICIO	DESCRIPCIÓN
AIM/New-ICQ (TCP:5190)	Servicio de Mensajería internet AOL, utilizado como puerto de escucha por ICQ.
BGP (TCP:179)	Border Gateway Protocol.
BOOTP_CLIENT (UDP:68)	Cliente DHCP
BOOTP_SERVER (UDP:67)	Servidor DHCP
DNS (UDP/TCP:53)	Domain Name Server, un servicio que hace corresponder nombres web con números IP
FTP(TCP:20,21)	File Transfer Protocol, programa que habilita un transferencia rápida de ficheros
H.323 (TCP:1720)	Protocolo utilizado por NetMeeting
HTTP (TCP:80)	Hyper Text Transfer Protocol – protocolo cliente/servidor para la navegación web
HTTPS (TCP:443)	HTTPS es una sesión http segura utilizada frecuentemente en el comercio electrónico
ICQ (UDP:4000)	Programa de chat en internet
IKE (UDP:500)	El algoritmo IKE es utilizado para la distribución y gestión de claves.
IPSEC_TUNNEL (AH:0)	El protocolo de tunelizado IPSEC AH utiliza este servicio
IPSEC_TUNNEL (ESP:0)	El protocolo de tunelizado IPSEC ESP utiliza este servicio
PING (ICMP:0)	Es el protocolo que envía paquetes ICMP para comprobar si un host remoto es o no alcanzable.
POP3 (TCP:110)	Este protocolo permite a un ordenador cliente el obtener un e-mail de un servidor POP3 a través de una conexión temporal.
PPTP (TCP:1723)	El protocolo PPTP posibilita la transferencia segura de datos sobre redes públicas. Este es el canal de control.
PPTP_TUNNEL (GRE:0)	El protocolo PPTP posibilita la transferencia segura de datos sobre redes públicas. Este es el canal de datos.
REAL_AUDIO (TCP:7070)	Un servicio de streaming de audio que posibilita la recepción de audio en tiempo real a través de la web.
SMTP (TCP:25)	Simple Mail Transfer Protocol es el estandar para el intercambio de mensajes a través de internet.

CAPÍTULO 10: RUTAS ESTÁTICAS

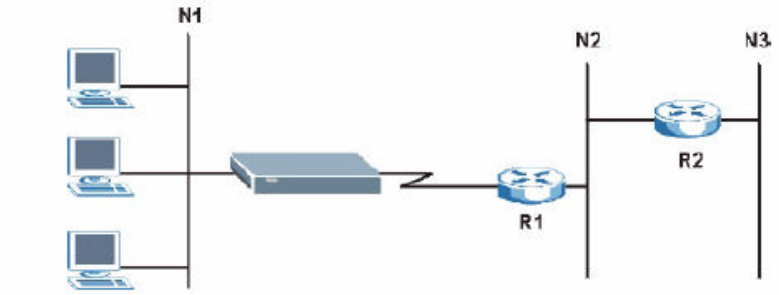
Este capítulo describe como configurar rutas estáticas en su P320W

10.1 Descripción de rutas estáticas

Las rutas estáticas indican al Prestige información de enrutamiento que no puede ser aprendida automáticamente a través de otros medios. Esto puede darse en casos en los que el RIP está deshabilitado en la LAN o cuando una red remota está más allá del nodo remoto al que se está directamente conectado.

Cada nodo remoto especifica sólo la red a la que el gateway está directamente conectado y el Prestige no tiene conocimiento de las redes que hay más allá. Por ejemplo, el Prestige tiene conocimiento de la red N2 de la siguiente figura a través del nodo remoto del Router 1. Sin embargo, el Prestige es incapaz de enlutar un paquete a la red N3 porque no conoce la existencia de una ruta a través del nodo remoto del Router 1 (a través del Router 2). Las rutas estáticas permiten darle a conocer al Prestige acerca de estas redes situadas más allá de los nodos remotos.

Figura 64 Ejemplo de Topología de Rutas Estáticas



10.2 Pantalla de Rutas Estáticas

Pulse sobre el enlace **Rutas estáticas IP** bajo las opciones de **Gestión** para abrir la pantalla **Rutas estáticas IP**. Se mostrará la siguiente pantalla.

Figura 65 Rutas estáticas IP

La siguiente tabla describe las etiquetas dentro de esta pantalla.

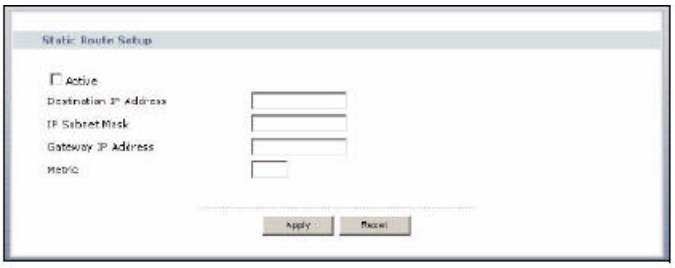
Tabla 49 Rutas Estáticas IP

ETIQUETA	DESCRIPCIÓN
#	Número de la ruta estática
Activa	Este icono está habilitado cuando la ruta estática está activada. Pulse sobre el icono de edición bajo **Modificar** y seleccione la casilla **Activar** en la pantalla de **Configuración de la Ruta Estática** para habilitar esta ruta. Desmarcar la casilla para deshabilitar esta ruta estática sin necesidad de eliminarla.
Destino	Este parámetro especifica la dirección IP de la red destino. El enrutamiento está basado en número de red.
Puerta de enlace	Este campo indica la dirección IP de la puerta de enlace. La puerta de enlace es un equipo conectado al gateway que enviará el paquete a su destino. En la LAN, la puerta de enlace deberá ser un router dentro del mismo segmento de LAN que el P320W; y sobre la WAN, la puerta de enlace deberá ser la dirección IP de alguno de los nodos remotos.
Modificar	Pulse sobre el icono **de edición** para abrir la pantalla de **Configuración de la ruta estática**. Modificar una ruta estática o crear una nueva regla en la pantalla de configuración. Pulse sobre el icono **de borrado** para eliminar una ruta estática.

10.2.1 Pantalla de Configuración de Ruta Estática

Para editar una ruta estática, pulsar sobre el icono de **edición** bajo **Modificar**. Aparecerá la siguiente pantalla. Complete la información requerida para cada ruta estática.

Figura 66 Configuración de ruta estática



La siguiente tabla describe las etiquetas de esta pantalla.

Tabla 50 Configuración de Ruta Estática

ETIQUETA	DESCRIPCIÓN
Activar	Este campo permite activar/desactivar la ruta estática
Dirección IP destino	Este parámetro especifica la dirección IP de red del destino.
Máscara de subred	Introduzca aquí la máscara de subred.
Dirección IP puerta de enlace	Introduzca aquí la dirección de la puerta de enlace.
Métrica	La métrica representa el "coste" de una transmisión. El enrutamiento IP utiliza los saltos para medir el coste, con un mínimo de 1 para redes conectadas directamente. Introduzca el número aproximado del coste de este enlace.
Aplicar	Pulse **Aplicar** para guardar los cambios.
Restaurar	Pulse **Restaurar** para volver a configurar esta pantalla de nuevo.

CAPÍTULO 11: GESTIÓN REMOTA

Este capítulo proporciona información sobre las pantallas de gestión remota

11.1 Descripción de la Gestión Remota

La gestión remota permite determinar a qué servicios/protocolos del Prestige es posible acceder, a través de qué interfaces y desde qué ordenadores.

Nota: Cuando se configura la gestión remota para permitir la gestión desde la WAN, es necesario configurar una regla en el firewall para permitir el acceso. Consulte el capítulo del firewall para más detalles sobre la configuración de reglas del firewall.

Es posible gestionar el P320W a través de:

- LAN Only (Sólo LAN) - Todos los interfaces (LAN y WAN)

Para deshabilitar la gestión remota de un servicio, seleccione **LAN** en el campo correspondiente del **Servidor de Acceso**.

11.1.1 Limitaciones de la Gestión Remota

La gestión remota sobre la LAN o la WAN no funcionará si:

1. Se ha deshabilitado el servicio en una de las pantallas de gestión remota.
2. La dirección IP del campo **Cliente IP de Confianza** no coincide con la dirección IP del cliente. Si no hay coincidencia, el P320W desconectará la sesión inmediatamente.
3. Hay una regla del firwall que está bloqueando este tráfico.

11.1.2 Gestión Remota y NAT

Cuando el NAT está habilitado:

• Utilice la dirección IP de la WAN del P320W cuando esté accediendo el equipo desde la WAN.

• Utilice la dirección IP de la LAN del P320W cuando esté accediendo desde la LAN.

11.1.3 Temporizador del Sistema

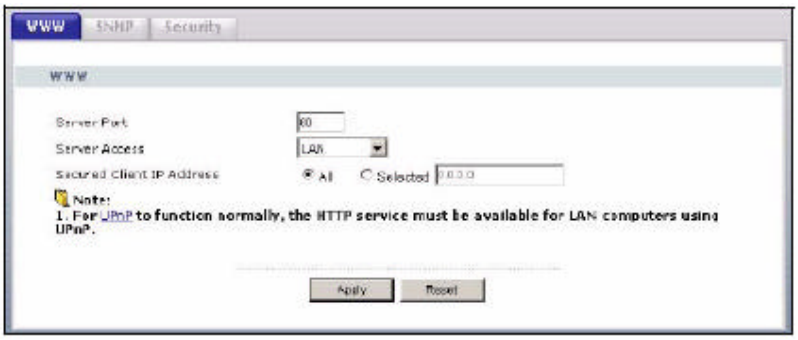
Hay un temporizador del sistema de cinco minutos (300 segundos). Su P320W le desconectará del sistema automáticamente si la sesión permanece inactiva durante ese periodo de tiempo, excepto cuando se está continuamente mostrando una

pantalla de estadísticas con refrescos periódicos. Es posible modificar este temporizador en la pantalla **Status (Estado).**

11.2 Pantalla WWW

Para modificar los parámetros de gestión http del P320W, pulse sobre el enlace **MGMT a distancia (Gestión remota)** bajo las opciones de **Gestión** para mostrar la pantalla **WWW**.

Figura 67 Gestión remota WWW



La siguiente tabla describe las etiquetas de esta pantalla.

Tabla 51 Gestión remota WWW

ETIQUETA	DESCRIPCIÓN
Puerto Servidor	Se deberá mantener el puerto establecido por defecto y únicamente modificarlo en caso de ser necesario.
Acceso al Servicio	Seleccione el interfaz (o interfaces) a través de los cuáles se permitirá comunicarse con el P320W utilizando este servicio.
Dirección IP de Cliente de Confianza	Un cliente de confianza es un ordenador al que le está permitido el acceso al gateway utilizando este servicio. Seleccione **Todos (All)** para permitir que cualquier ordenador pueda acceder al gateway utilizando este servicio. Escoja **Selectivo (Selected)** para permitir que únicamente el ordenador cuya dirección IP coincida con la especificada pueda acceder al P320W utilizando este servicio.
Aplicar	Pulse **Aplicar** para guardar los cambios
Resetear	Pulse **Resetear** para volver a configurar la pantalla de nuevo.

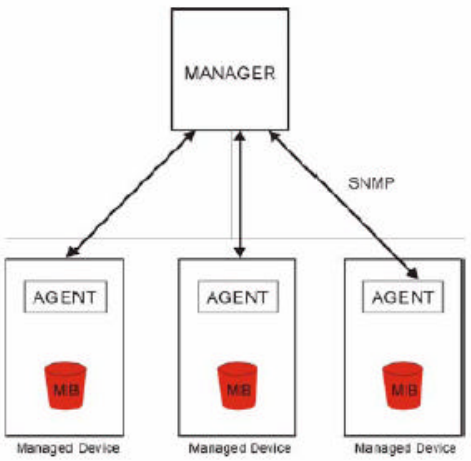
11.3 SNMP

SNMP (Simple Network Management Protocol – Protocolo de Gestión de Red Simple) es un protocolo utilizado para intercambiar información de gestión entre dispositivos de red. SNMP es un miembro del conjunto de protocolos TCP/IP.

El Prestige soporta la funcionalidad de agente SNMP, lo que permite a una máquina de gestión el controlar y monitorizar el Prestige a través de la red. El Prestige soporta

la versión 1 SNMP (SNMPv1) y la versión dos c (SNMPv2c). La siguiente figura ilustra una operación de gestión SNMP. SNMP únicamente estará disponible si el TCP/IP está configurado.

Figura 68 Modelo de Gestión SNMP



Una red gestiona SNMP consiste en dos componentes principales: agentes y un gestor.

Un agente es un módulo software de gestión que reside en un dispositivo gestionado (el Prestige). Un agente traduce la información de gestión local del dispositivo gestionado a una forma compatible con SNMP. El administrador es la consola a través de la cual los administradores de red llevan a cabo las funciones de gestión de la red. Ejecuta aplicaciones que controlan y monitorizan los dispositivos gestionados.

Los dispositivos gestionados contienen variables objeto que definen cada parte de información que será recogida sobre un dispositivo. Ejemplos de variables serían el número de paquetes recibidos, el estado del puerto del nodo, etc. Una base de información de gestión (Management Information Base, MIB) es un conjunto de variables objeto. SNMP permite al administrador y a los agentes comunicarse para acceder a estos objetos.

SNMP en sí mismo es un simple protocolo petición/respuesta basado en el modelo administrador/agente. El administrador emite una petición y el agente da una respuesta a través del siguiente protocolo de operaciones:

• Get - Permite al administrador recuperar una variable objeto del agente.

• GetNext – Permite al administrador recuperar la siguiente variable objeto de una tabla o lista dentro de un agente. En SNMPv1, cuando un administrador quiere

recuperar todos los elementos de una tabla de un agente, empieza con una operación Get, seguida de una serie de operaciones GetNext.

• Set – Permite al administrador configurar valores para las variables dentro de un agente.

• Trap - Usado por el agente para informar al administrador sobre algunos eventos.

11.3.1 MIBs soportadas

El Prestige soporta RFC-1215 y MIB II como se define en la RFC-1213 así como las MIBs privadas de ZyXEL. El foco de las MIBs es permitir a los administradores el recoger datos estadísticos y monitorizar el estado y funcionamiento.

11.3.2 Traps SNMP

El Prestige enviará traps al gestor SNMP cuando se produzca alguno de los siguientes eventos:

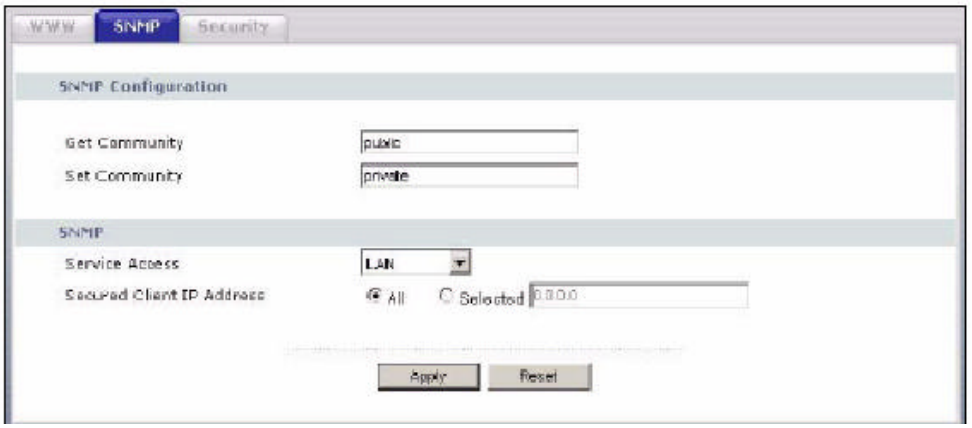
Tabla 52 Traps SNMP

TRAP #	NOMBRE TRAP	DESCRIPCIÓN
1	coldStart (definido en RFC-1215)	Se envía un trap después de iniciar (encendido).
2	warmStart (definido en RFC-1215)	Se envía un trap después de reiniciar (reinicio de software).
3	linkDown (definido en RFC-1215)	Trap que se envía con el número de puerto cuando cualquier de los enlaces está caído. Vea la siguiente tabla.
4	linkUp (definido en RFC-1215)	Se envía un trap con el número de puerto.
5	authenticationFailure (definido en RFC-1215)	Se envía un trap al administrador cuando se recive un SNMP get o set con la comunidad (contraseña) errónea.
6	whyReboot (definido en RFC-1215)	Se envía un trap con la razón del reinicio antes de que el sistema vaya a reiniciarse (inicio en caliente).
6a	For intentional reboot:	Se envía un trap con el mensaje "System reboot by user!" si el reinicio se hace intencionadamente, (por ejemplo, descarga de nuevos ficheros, Comando "sys reboot", etc.).

11.4 Pantalla SNMP

Para modificar los parámetros SNMP del P320W, pulse sobre el enlace MGMT a distancia (Gestión remota) bajo las opciones de Gestión y seleccione la pestaña SNMP. Aparecerá la siguiente pantalla.

Figura 69 Gestión remota SNMP



La siguiente tabla describe las etiquetas de esta pantalla.

Tabla 53 Gestión remota SNMP

ETIQUETA	DESCRIPCIÓN
Configuración SNMP	
Comunidad de Lectura	Introduzca la comunidad de lectura, que será la contraseña para las peticiones Get y GetNext que se reciban desde la estación de gestión. Por defecto es pública y permite todas las peticiones.
Comunidad de Escritura	Introduzca la comunidad de escritura, que será la contraseña para las peticiones Set recibidas desde la estación de gestión. Por defecto es pública y permite todas las peticiones
SNMP	
Acceso al Servicio	Seleccione el interfaz (o interfaces) a través de los cuáles se permitirá el acceso al P320W utilizando este servicio.
Dirección IP de Cliente de Confianza	Un cliente de confianza es un ordenador al que le está permitido el acceso al gateway utilizando este servicio. Seleccione **Todos (All)** para permitir que cualquier ordenador pueda acceder al gateway utilizando este servicio. Escoja **Selectivo (Selected)** para permitir que únicamente el ordenador cuya dirección IP coincida con la especificada pueda acceder al P320W utilizando este servicio.
Aplicar	Pulse **Aplicar** para guardar los cambios
Resetear	Pulse **Resetear** para volver a configurar la pantalla de nuevo.

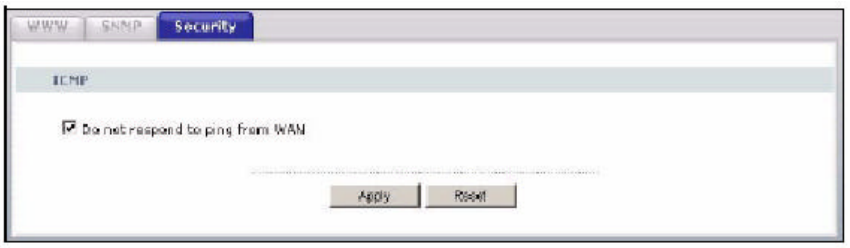
11.5 Pantalla Seguridad

Para modificar los parámetros de seguridad de su P320W, pulse sobre el **enlace MGMT a distancia (Gestión remota)** bajo las opciones de **Gestión** y seleccione la pestaña **Seguridad**. La pantalla que a parecerá será la siguiente.

Si algún usuario externo intenta acceder a un servicio no soportado por su P320W, se generará un paquete ICMP de respuesta automáticamente.Esto permite al usuario externo el conocer la existencia del P320W. El equipo P320W soporta la funcionalidad anti-probing, la cuál previene que estos paquetes ICMP de respuesta sean enviados.

Esto evita que cualquier usuario externo puede descubrir la existencia de su equipo cuando se comprueban puertos no utilizados.

Figura 70 Seguridad de Gestión Remota



La siguiente tabla describe las etiquetas dentro de esta pantalla.

Tabla 54 Seguridad de la Gestión Remota

ETIQUETA	DESCRIPCIÓN
ICMP	El protocolo ICMP es un protocolo basado en mensajes de control e informes de error entre un host servidor y un gateway en internet.
No responder a ping recibidos desde la WAN	El P320W no responderá a ninguna petición Ping entrante en la WAN cuando se marque esta opción.
Aplicar	Pulse **Aplicar** para guardar los cambios.
Resetear	Pulse **Resetear** para volver a configurar esta pantalla de nuevo.

CAPÍTULO 12: UPNP

Este capítulo introduce la funcionalidad Universal Plug and Play

12.1 Descripción del Universal Plug and Play

Universal Plug and Play (UPnP) es un estándar distribuido, abierto que utiliza TCP/IP para la conectividad entre dispositivos. Un dispositivo UPnP puede unirse dinámicamente a una red, obtener una dirección IP, compartir sus capacidades y aprender acerca de otros dispositivos de la red. Adicionalmente, un dispositivo puede dejar una red automáticamente cuando no se encuentre en uso.

12.1.1 ¿Cómo saber si se está utilizando UPnP?

El hardware UPnP se identifica con un icono en la carpeta de Conexiones de Red (Windows XP). Cada dispositivo UPnP compatible instalado en la red aparecerá con un icono separado. Seleccionando el icono de un dispositivo UPnP podrá acceder a la información y propiedades del mismo.

12.1.2 NAT Traversal

UPnP NAT Traversal automatiza el proceso de permitir a una aplicación operar a través del NAT. Los dispositivos de red UPnP pueden configurar automáticamente el direccionamiento de red, anunciar su presencia en la red a otros dispositivos UPnP y habilitar el intercambio de descripciones de servicio sencillas. El NAT Traversal ofrece lo siguiente:

1. Mapeo de puertos dinámico
2. Aprendizaje de direcciones IP públicas
3. Asignación de temporizadores a los mapeos.

Windows Messenger es un ejemplo de aplicación que soporta NAT Traversal y UPnP. Consulte el capítulo NAT para más información sobre la misma.

12.1.3 Precauciones con UPnP

La naturaleza automática de las aplicaciones NAT Traversal para establecer sus propios servicios y abrir los puertos del firewall puede presentar problemas de

seguridad en las redes. La información de red y la configuración podría ser obtenida y modificada por usuarios en algunos entornos de red.

Todos los dispositivos con UPnP habilitado podrán comunicarse libremente entre ellos sin ninguna configuración adicional. Deshabilite el UPnP si ésta no es su intención.

12.2 UPnP y ZyXEL

ZyXEL ha logrado la certificación UPnP del Universal Plug and Play Forum Creates UPnPTM Implementers Corp. (UIC).

La implementación UPnP de ZyXEL soporta IGD 1.0 (Internet Gateway Device). En el momento de escribir este documento la implementación UPnP de ZyXEL soporta Windows Messenger 4.6 y 4.7 mientras que el Windows Messenger 5.0 y XBOX están todavía en pruebas.

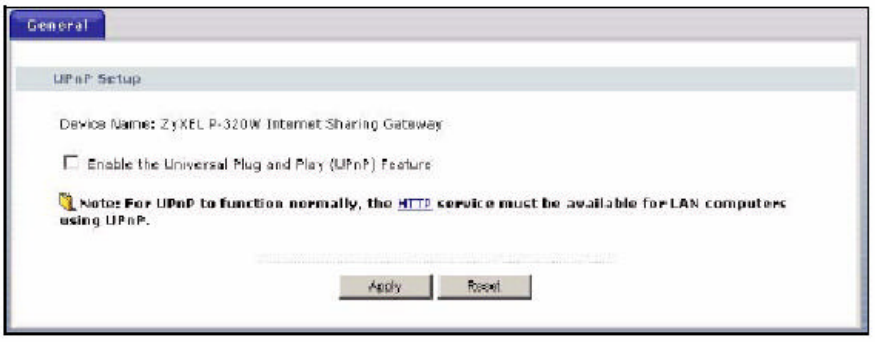
El broadcast UPnP sólo está permitido en la LAN.

Consulte secciones posteriores para ver ejemplos sobre la instalación del UPnP en Windows XP y Windows Me así como un ejemplo del uso del UPnP en Windows.

12.3 Pantalla UPnP

Pulse sobre el enlace **UPnP** bajo las opciones de **Gestión** para mostrar la pantalla UPnP.

Figura 71 Configuración UPnP



La siguiente tabla describe las etiquetas dentro de esta pantalla.

Tabla 55 Configuración del UPnP

ETIQUETA	DESCRIPCIÓN
Habilitar la funcionalidad Universal Plug and Play (UPnP)	Seleccione esta casilla para activar el UPnP. Tenga la precaución de que cualquiera podrá utilizar la aplicación UPnP para abrir la pantalla de acceso del configurador web sin introducir la dirección IP del Prestige (aunque todavía será necesario introducir la contraseña para acceder al configurador web).
Aplicar	Pulse **Aplicar** para guardar los cambios.
Resetear	Pulse **Resetear** para volver a los parámetros previamente almancenados.

12.4 Ejemplo de Instalación UPnP en Windows

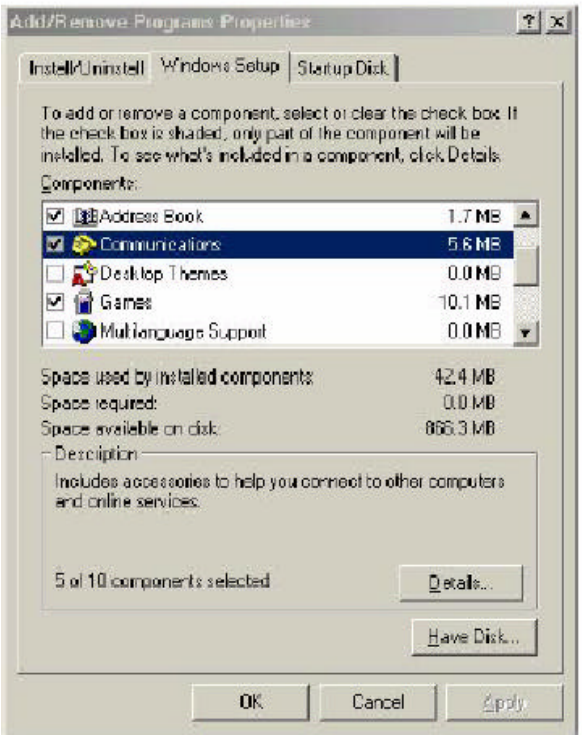
Esta sección muestra como instalar UPnP en Windows Me y Windows XP.

12.4.1 Instalación UPnP en Windows Me

1. Pulse **Inicio** y **Panel de Control**. Doble-click en **Agregar/Quitar programas.**

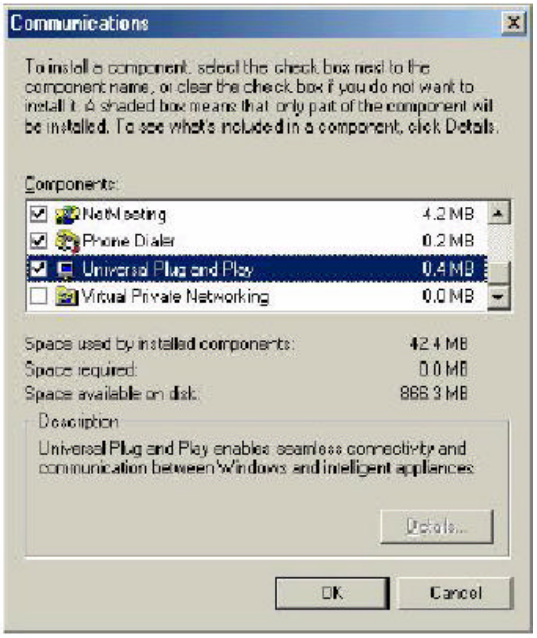
2. Pulse en la pestaña de **Configuración de Windows** y seleccione **Comunicaciones** en la casilla de selección de **Componentes**. Pulse **Detalles.**

Figura 72 Añadir/Quitar Programas: Configuración Windows: Comunicaciones



3. En la pantalla **Comunicaciones**, seleccione la casilla **Universal Plug and Play** en la caja de **Componentes**.

Figura 73 Añadir/Quitar Programas: Configuración Windows: Comunicaciones: Componentes



4. Pulse sobre **Aceptar** para volver a la pantalla de Propiedades de Agregar/Quitar Programas y pulse sobre **Siguiente**.

5. Reinicie el ordenador cuando se le pida.

12.4.2 Instalación UPnP en Windows XP

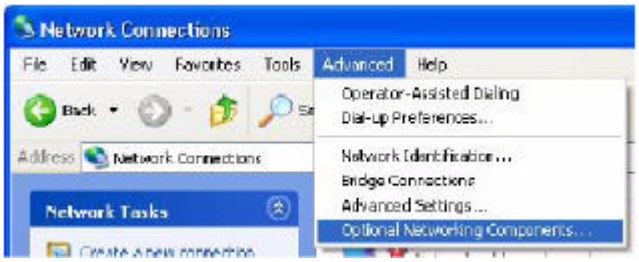
Siga los siguientes pasos para instalar UPnP en Windows XP.

1. Pulse **Inicio** y **Panel de Control.**

2. Haga doble clic en **Conexiones de Red.**

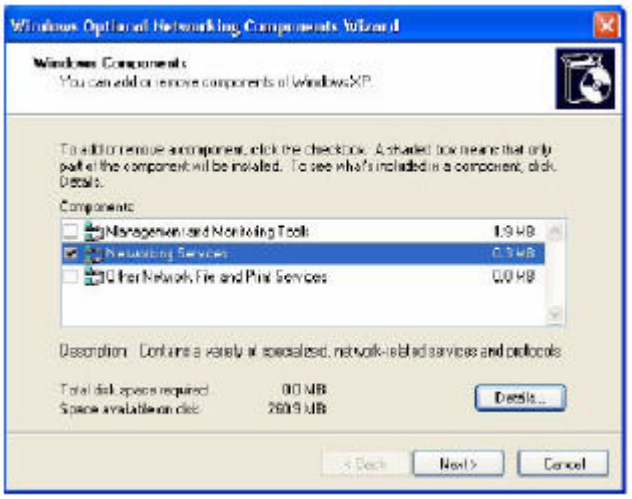
3. En la ventana de **Conexiones de Red**, pulse sobre **Opciones Avanzadas** en el menú principal y seleccione **Componentes de Red Opcionales…** Se mostrará la ventana del **Asistente de Componentes Opcionales de Red**.

Figura 74 Conexiones de red



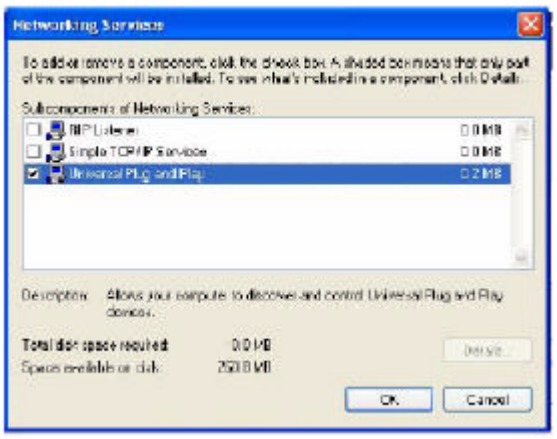
4. Seleccione **Servicios de Red** en la caja de selección de **Componenetes** y pulse sobre **Detalles.**

Figura 75 Asistente de Windows para los componentes opcionales de red



5. En la ventana de **Servicios de Red**, seleccione la casilla de **Universal Plug and Play.**

Figura 76 Servicios de red



6. Pulse **Aceptar** para volver a la ventana del **Asistente de Componentes Opcionales de Red** y pulse **Siguiente.**

12.5 Ejemplo de Utilización de UPnP en Windows XP

Esta sección muestra como utilizar la funcionalidad UPnP en Windows XP. Debe disponer del UPnP instalado enWindows XP y activado en el Prestige.

Igualmente asegúrese que el ordenador está conectado al puerto LAN del Prestige. Encienda su ordenador y el Prestige.

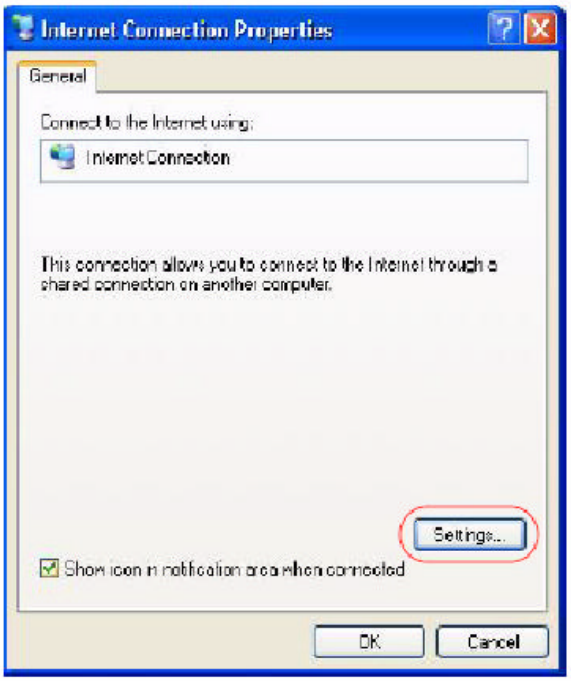
12.5.1 Auto-descubrir dispositivos de red UPnP

1. Pulse sobre **Inicio** y **Panel de Control**. Doble-click en **Conexiones de Red**. Un icono aparecerá en el apartado de Puerta de enlace de Internet.
2. Pulse con el botón derecho del ratón en el icono y seleccione **Propiedades.**

Figura 77 Conexiones de red

3. En la ventana de **Propiedades de Conexión a Internet**, pulse sobre **Configuración** para ver los mapeos de puertos que han sido creados automáticamente.

Figura 78 Propiedades de conexión a Internet



4. Deberá editar o borrar el mapeo de puertos o pulsar sobre **Agregar** para añadir mapeos de puertos manualmente.

Figura 79 Propiedades de conexión a Internet: Parámetros avanzados

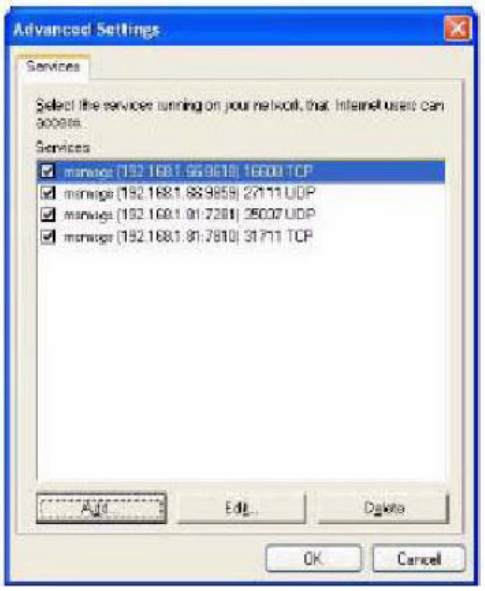
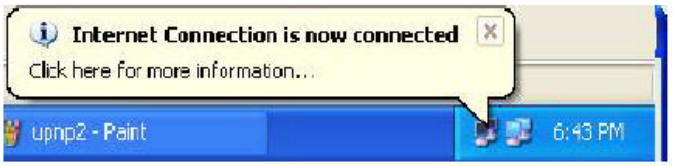


Figura 80 Propiedades de conexión a Internet: Parámetros avanzados: Añadir

5. Cuando el dispositivo UPnP sea desconectado de su ordenador, todos los mapeos serán borrados automáticamente.

6. Seleccione la opción **Mostrar icono en el área de notificación al conectarse** y pulse **Aceptar**. Un icono aparecerá en la barra de tareas del sistema

Figura 81 Icono del sistema



7. Haga doble clic en el icono para mostrar el estado de la conexión a Internet actual.

Figura 82 Estado de la conexión a Internet

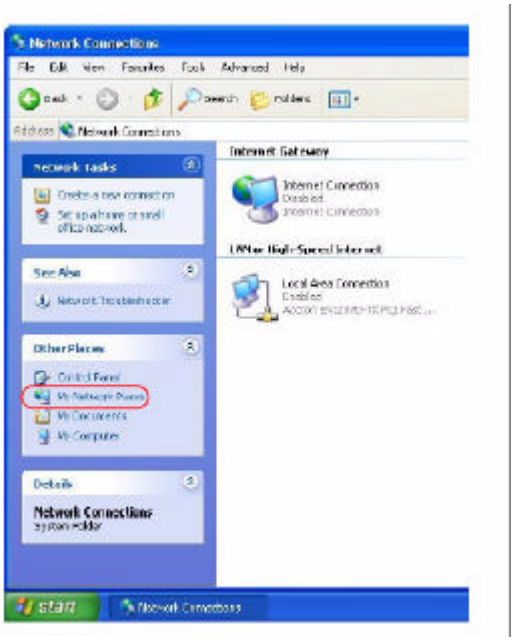
12.5.2 Configurador web de fácil acceso

Con UPnP, es posible acceder al configurador basado en web del Prestige sin necesidad de conocer la dirección IP del Prestige. Esto es útil en caso de desconocimiento de la dirección IP del Prestige.

Siga los siguientes pasos para acceder al configurador web.

1. Pulse sobre **Inicio** y **Panel de Control.**
2. Haga doble clic en **Conexiones de Red.**
3. Seleccione **Mis Sitios de Red** bajo **Otros sitios.**

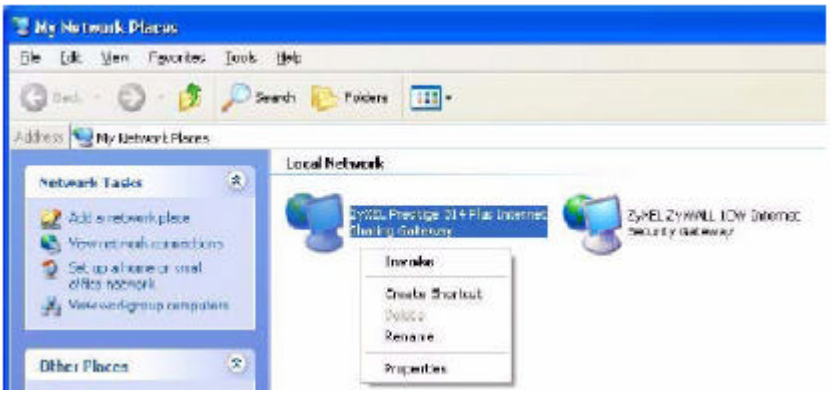
Figura 83 Conexiones de red



4. Un icono con la descripción de cada dispositivo UPnP se muestra bajo **Red Local.**

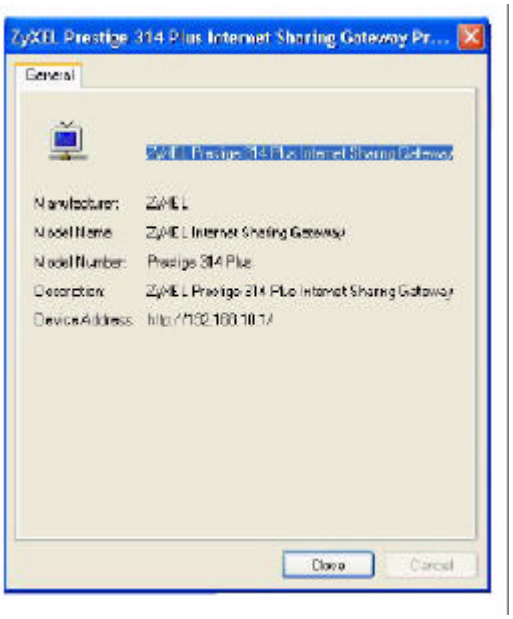
5. Pulse con el botón derecho del ratón en el icono del Prestige y seleccione **Abrir**. La pantalla de acceso al configurador web aparecerá.

Figura 84 Conexiones de red : Mis sitios de red



6. Pulse con el botón derecho del ratón de su P320W y seleccione **Propiedades**. Una ventana de propiedades aparecerá con información básica del gateway.

Figura 85 Conexiones de red : Mis sitios de red : Propiedades : Ejemplo



CAPÍTULO 13: SISTEMA

Este capítulo proporciona información sobre las pantallas del sistema

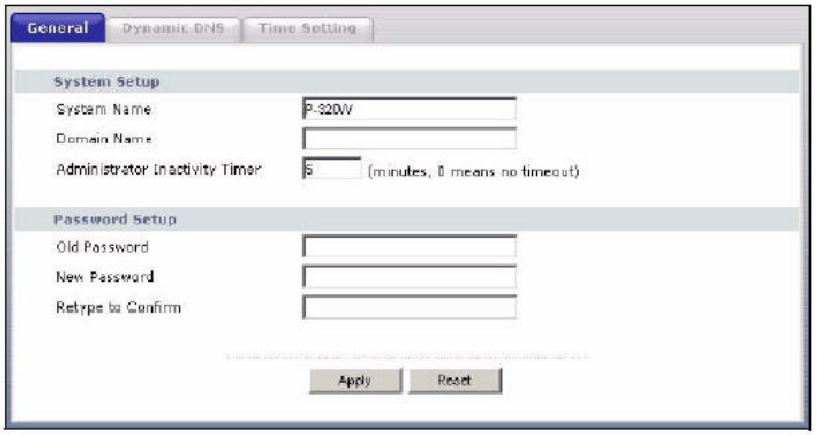
13.1 Descripción del Sistema

Consulte el capítulo del Asistente de Configuración para obtener más información sobre las próximas pantallas.

13.2 Pantalla General

Pulse sobre el enlace Sistema bajo las opciones de Mantenimiento y seleccione la pestaña General. Se mostrará la siguiente pantalla.

Figura 86 Sistema General



La siguiente tabla describe las etiquetas dentro de esta pantalla.

Tabla 56 Sistema General

ETIQUETA	DESCRIPCIÓN
Nombre del Sistema	El nombre del sistema es un nombre único para identificar al P320W dentro de la red.El nombre podrá disponer de hasta 30 caracteres alfanuméricos.
Nombre de dominio	Introduzca el nombre de dominio aquí. Si deja este campo en blanco, el ISP deberá asignarle un nombre de dominio a través de DHCP. El nombre de dominio introducido aquí tendrá mayor prioridad que el que pueda recibir de su ISP.
Temporizador de inactividad	Introduzca el número de minutos que una sesión de gestión podrá permanecer sin tráfico antes de ser desconectada. Por defecto son 5 minutos. Un valor "0" indica que la sesión de gestión nunca expira, sin importar el tiempo que permanezca inactiva (no es recomendable esta opción).
Configuración de contraseña	Modifique la contraseña de su P320W (recomendado) utilizando este campo.

Contraseña antigua	Introduzca la contraseña actual utilizada para acceder al router.
Contraseña nueva	Introduzca la nueva contraseña que desea utilizar
Volver a introducir para confirmar	Vuelva a introducir la nueva contraseña en este campo.
Aplicar	Pulse **Aplicar** para guardar los cambios.
Resetear	Pulse **Resetear** para volver a configurar esta pantalla de nuevo.

13.3 DNS Dinámico

La funcionalidad del DNS Dinámico le permite actualizar su dirección IP pública dinámica con uno o varios nombres de dominio de manera que cualquiera pueda acceder a su dispositivo (utilizando NetMeeting, etc.) Igualmente se podrá acceder a un servidor FTP o sitio Web instalados en su propio ordenador utilizando un nombre de dominio (por ejemplo myhost.dhs.org, donde myhost es un nombre a elegir) que nunca cambiará en lugar de una dirección IP dinámica que puede cambiar cada vez que se conecte. A sus amigos o conocidos siempre les será posible contactar con usted aunque no tengan conocimiento de cuál es la IP pública que tiene asignada.
En primer lugar, necesitará tener registrada una cuenta DNS dinámica en www.dyndns.org. Esto será útil para personas con una dirección IP dinámica suministrada por su ISP. El proveedor de servicio DNS Dinámico le proporcionará una clave o contraseña

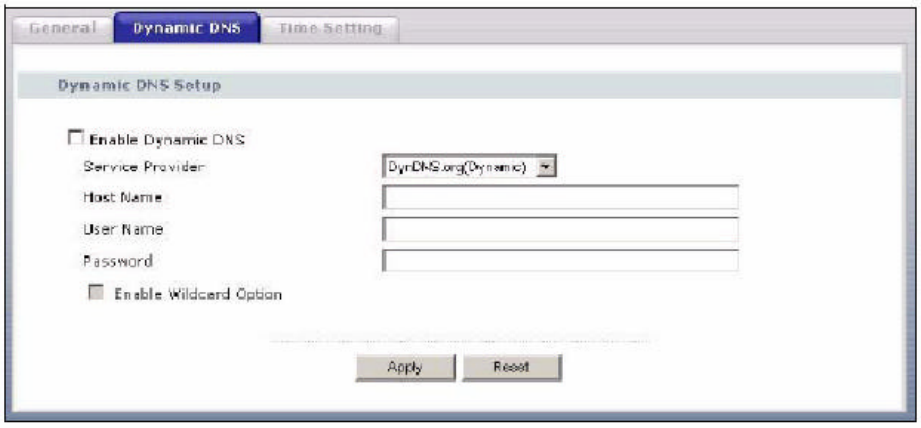
13.3.1 Wildcard DynDNS

Habilitando la funcionalidad wildcard para su máquina hará que *.yourhost.dyndns.org sea asociado a la misma dirección IP que yourhost.dyndns.org. Esta funcionalidad es útil si se desea utilizar, por ejemplo, www.yourhost.dyndns.org y a la vez seguir pudiendo alcanzar el propio equipo.
Nota: Si dispone de una dirección IP privada en la WAN, no podrá utilizar la funcionalidad DNS Dinámica.

13.4 Pantallas DNS Dinámico

Para modificar los parámetros del DNS Dinámico del P320W, pulse sobre el enlace Sistema bajo las opciones de Mantenimiento y seleccione la pestaña DNS Dinámcio. Le aparecerá la siguiente pantalla.

Figura 87 DNS Dinámico



La siguiente tabla describe las etiquetas dentro de esta pantalla.

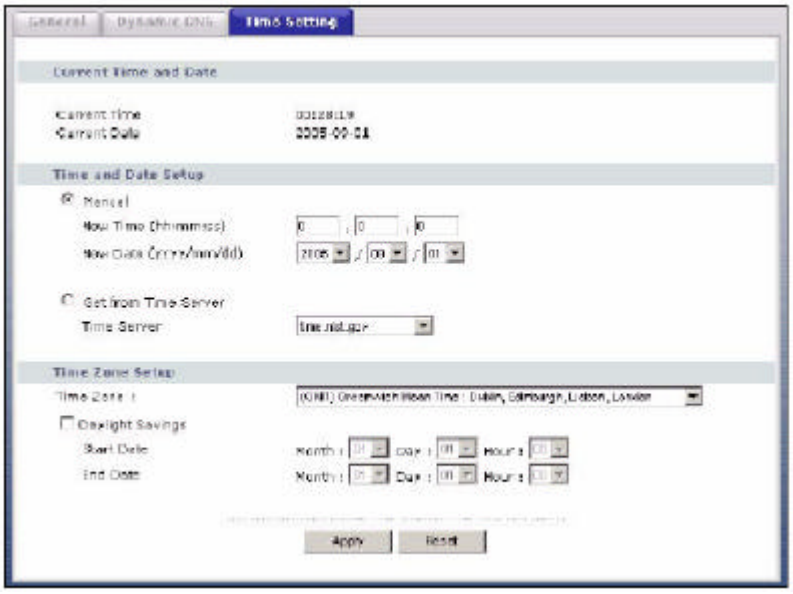
Tabla 57 DNS Dinámico

ETIQUETA	DESCRIPCIÓN
Habilitar DNS Dinámico	Seleccione esta casilla para utilizar el DNS Dinámico.
Proveedor del servicio	Seleccione el nombre de su proveedor de servicio DNS Dinámico.
Nombre del Host	Introduzca el nombre del host en este campo.
Nombre de usuario	Introduzca su nombre de usuario.
Contraseña	Introduzca la contraseña asignada.
Habilitar la opción Wildcard	Seleccione esta casilla para habilitar la Wildcard DynDNS
Aplicar	Pulse **Aplicar** para guardar los cambios.
Resetear	Pulse **Resetear** para volver a configurar la pantalla de nuevo.

13.5 Pantalla de Configuración de Fecha/Hora

Para modificar los parámetros de fecha/hora de su P320W, pulse sobre el enlace **Sistema** bajo las opciones de **Mantenimiento** y seleccione la pestaña **Servidor de Tiempo**. Aparecerá una pantalla como la siguiente. Utilice esta pantalla para configurar la ho ra de su P320W en base a su zona horaria.

Figura 88 Parámetros de Tiempo



La siguiente tabla describe las etiquetas dentro de esta pantalla.

Tabla 58 Parámetros de Tiempo

ETIQUETA	DESCRIPCION
Fecha y hora actuales	
Hora actual	Este campo muestra la hora de su router. Cada vez que se cargue esta página, el P320W sincronizará la hora con el servidor de tiempo.
Fecha actual	Este campo muestra la fecha de su router. Cada vez que se cargue esta página, el P320W sincronziará la fecha con el servidor de tiempo.
Configuración de Fecha y Hora	
Manual	Seleccione esta casilla para introducir los parámetros de tiempo de forma manual. Si se configura una nueva fecha y hora, zona horaria y horario de verano de forma simultánea, la nueva fecha y hora introducidas tendrán prioridad de manera que no se verá afectada ni por la zona horaria ni por el horario de verano.
Nueva Hora (hh:mm:ss)	Este campo muestra la última hora actualizada desde el servidor de tiempo o la última hora configurada manualmente. Cuando se configura el modo **Manual**, introduzca en este campo la nueva hora y pulse **Aplicar.**
Nueva Fecha (yyyy-mm-dd)	Este campo muestra la última fecha actualizada recibida del servidor de tiempo o la última fecha configurada manualmente. Cuando se configura el modo **Manual**, introduzca en este campo la nueva fecha y pulse **Aplicar**.
Obtener los parámetros de un Servidor de Tiempo	Seleccione esta casilla para que su P320W obtenga la fecha y hora desde un servidor de tiempo que se especifique a continuación.

Servidor de Tiempo	Introduzca la dirección IP o el nombre de dominio del servidor de tiempo. Compruebe con ISP/administrador de red si no está seguro de esa información.
Configuración Zona Horaria	
Zona Horaria	Seleccione la zona horaria de su localización. Será configurada en función de su diferencia con la zona GMT.
Horario de Verano	El horario de verano es el periodo comprendido entre principios de primavera y principios de otoño que se aplica en varios países para proporcionar una hora más de día durante la tarde-noche.
Fecha de comienzo	Si usa ajuste horario de verano automático, introduzca el mes y día que comienza. El campo **Hora** en formato de 24 horas.
Fecha de finalización	Si usa ajuste horario de verano automático, introduzca el mes y día que finaliza. El campo **Hora** en formato de 24 horas.
Aplicar	Pulse **Aplicar** para guardar los cambios.
Resetear	Pulse **Resetear** para volver a configurar esta pantalla de nuevo.

CAPÍTULO 14: LOGS

Este capítulo contiene información sobre la configuración general de registro y visualización de logs en su P320W.

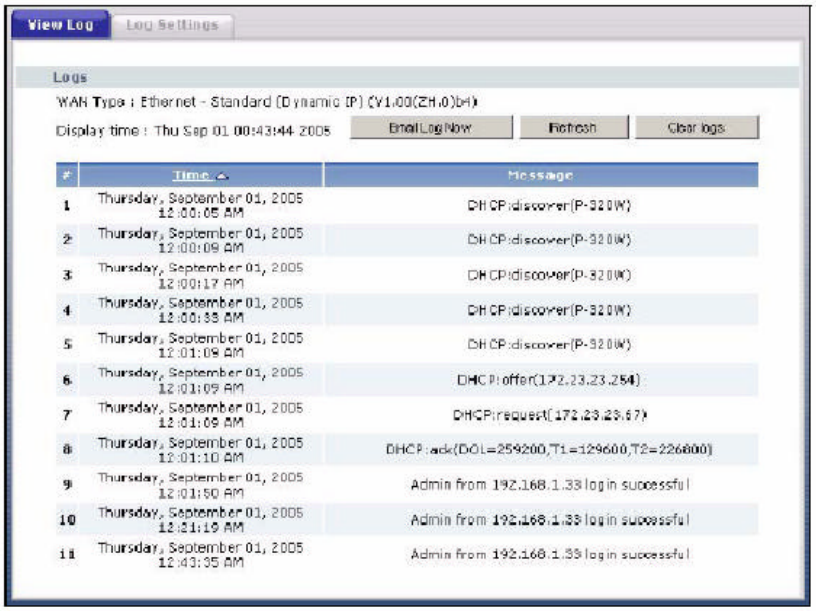
14.1 Visualización de Logs

El configurador Web permite visualizar todos los Logs del P320W en una única localización.

Pulse sobre el enlace **Logs** bajo las opciones de **Mantenimiento** para abrir la pantalla de **Visualización de Log.**

Las entradas en el registro en color rojo indican un error de sistema. Las entradas en el registro van rotando y borrando a las antiguas cuando el espacio disponible se llena. Pulse la cabecera de una columna para ordenar las entradas. Un triángulo indica que el ordenamiento se ha realizado en sentido ascendente o descendente.

Figura 89 Visualización de Log



La siguiente tabla describe las etiquetas dentro de esta pantalla.

Tabla 59 Visualización de log

ETIQUETA	DESCRIPCIÓN
Tipo de WAN	Este campo muestra el método de encapsulación (y tipo de servicio) que utiliza el P320W y la versión de firmware.
Tiempo de refresco	Este campo muestra cada cuanto tiempo se refresca esta pantalla.
Enviar Log por email ahora	Pulse sobre este botón para enviar la pantalla de logs a la dirección de email especificada en la página de **Configuración de Log**.
Refrescar	Pulse **Refrescar** para renovar la pantalla de logs.
Limpiar logs	Pulse este botón para borrar todos los logs.
Tiempo	Este campo muestra el tiempo en el que el log fue registrado. Consulte el capítulo de configuración de tiempo para configurar la fecha y hora de su router.
Mensaje	Este campo muestra el motivo del log.

14.2 Configuración de Logs

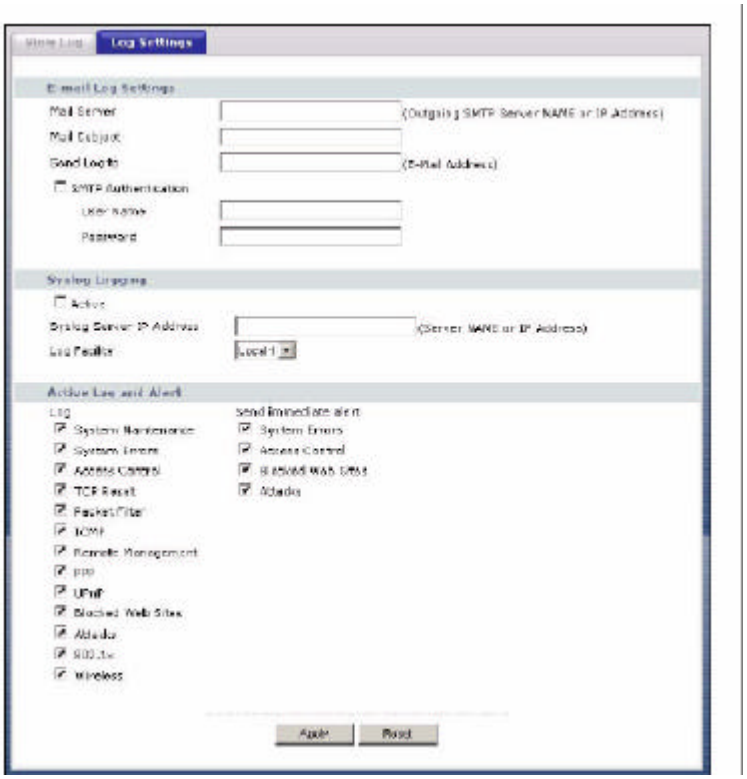
Puede configurar los parámetros generales de Logs del P320W en una única pantalla. Pulse sobre el enlace Logs bajo las opciones de Mantenimiento en el panel de navegación y la pestaña Parámetros de Logs para abrir la pantalla siguiente.

Utilice esta pantalla para configurar donde debe enviar los Logs el P320W; el horario sobre cuándo deben ser enviados y qué tipo de Logs y/o alertas deben ser remitidos.

Una alerta es un tipo de Log que requiere una atención más seria. Estos incluyen errores del sistema, ataques (control de acceso) e intentos de acceso a sitios Web bloqueados o sitios Web con restricción de funcionalidades Web como cookies, active X,…. Algunas categorías tales como los **Errores del Sistema** consisten tanto en Logs como en alertas. Se podrán diferenciar por el color en la pantalla de la **Visualización de Logs**. Las alertas aparecen en rojo y los Logs en negro.

Las alertas son remitidas por e-mail tan pronto como ocurren. Los Logs deben ser enviados tan pronto como el registro esté lleno. Seleccionando el envío de muchas alertas y/o Logs (especialmente de **Control de Acceso**) puede resultar en el envío de gran cantidad de e-mails.

Figura 90 Parámetros de Logs



La siguiente tabla describe las etiquetas dentro de esta pantalla.

ETIQUETA	DESCRIPCIÓN
Parámetros de E-mail para Logs	
Servidor de Correo	Introduzca el nombre del servidor o dirección IP del servidor de correo para las direcciones de correo especificadas más abajo. Si el campo se deja en blanco, los logs y las alertas no serán enviados por e-mail.
Asunto del Correo	Introduzca un título que desea aparezca en la línea de asunto de los mensajes de correo con logs que envíe el P320W.
Enviar el Log a	El P320W envía los logs a la dirección de e-mail que se especifique en este campo. Si el campo se deja en blanco, el P320W no enviará ningún log via e-mail.
Autenticación SMTP	SMTP (Simple Mail Transfer Protocol) es un estandar de intercambio de mensajes para internet. Seleccione esta casilla para activar la autenticación SMTP. Si se necesita autenticación del servidor de correo pero esta funcionalidad está deshabilitada, no se recibirán correos de logs.
Nombre de Usuario	Introduzca el nombre de usuario (hasta 31 caracteres) (normalmente el nombre de usuario de la cuenta de correo).

Contraseña	Introduzca la contraseña asociada con el nombre de usuario anterior.
Syslog	El P320W puede enviar el log a un servidor syslog externo.
Activar	Seleccione esta casilla para habilitar este envío.
Dirección IP servidor syslog	Introduzca la dirección IP o el nombre del servidor de syslog que registrará las categorías de logs seleccionadas.
Facilidad Log	Seleccione la localización de la lista desplegable. La facilidad de log permite registrar los mensajes en diferentes ficheros dentro del servidor syslog.
Activar Logs y Alertas	
Log	Seleccionar las categorías de logs que se desean registrar.
Enviar Alertas de forma inmediata	Seleccione las categorías de logs para las que el P320W enviará e-mails con alertas inmediatamente.
Aplicar	Pulse **Aplicar** para guardar los cambios.
Resetear	Pulse **Resetear** para volver a configurar la pantalla de nuevo.

CAPÍTULO 15: HERRAMIENTAS

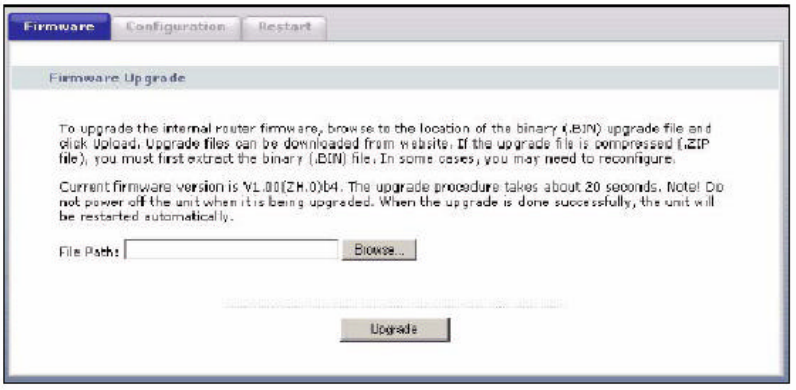
Este capítulo muestra como actualizar un nuevo firmware, actualizar o guardar el fichero de configuración y reiniciar su router

15.1 Pantalla de Actualización de Firmware

Podrá encontrar cualquier nuevo firmware para su dispositivo en la página www.zyxel.com en un fichero con extensión .bin dentro de un fichero comprimido. El proceso de carga utiliza http y puede tardar un par de minutos. Tras la actualización, el sistema se reiniciará.

Pulse sobre el enlace **Herramientas** dentro de las opciones de **Mantenimiento** dentro del panel de navegación. Siga las instrucciones de esta pantalla para actualizar el firmware en su router.

Figura 91 Actualización de Firmware



La siguiente tabla describe las etiquetas dentro de esta pantalla.

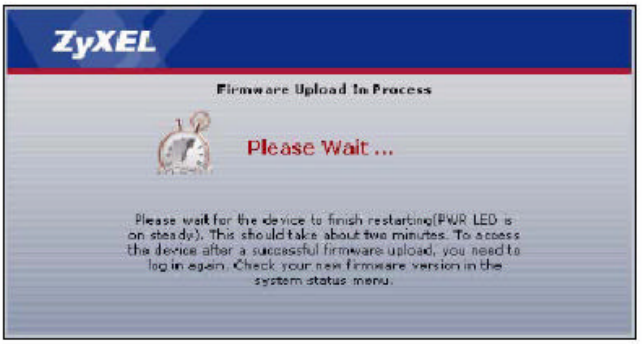
Tabla 61 Actualización de Firmware

ETIQUETA	DESCRIPCIÓN
Localización del fichero	Introduzca la localización del fichero que desea actualizar en este campo o pulse **Explorar…** para encontrarlo.
Explorar…	Pulse sobre el botón **Explorar…** para localizar el fichero .bin que quiere cargar.
Actualizar	Pulse sobre **Actualizar** para comenzar el proceso. El proceso de actualización puede llevar unos dos minutos.

Nota: No apague el P320W mientras el proceso de actualización está en progreso.

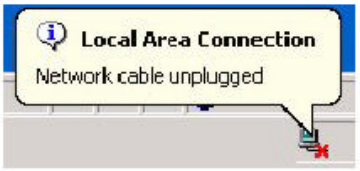
Tras visualizar la pantalla de **Actualización de Firmware en Progreso**, espere dos minutos antes de intentar acceder nuevamente a su P320W.

Figura 92 Aviso de Actualización



El P320W se reiniciará automáticamente originando una desconexión de red temporal. En algunos sistemas operativos, podría observar el siguiente icono en su escritorio.

Figura 93 Desconexión de red temporal



Tras dos minutos, vuelva a acceder de nuevo y compruebe que la nueva versión de firmware está cargada en la pantalla **Status (Estado).**

Si el proceso de actualización no se completa satisfactoriamente, aparecerá la siguiente ventana. Pulse sobre **Volver** para pasar nuevamente a la pantalla de **Firmware**.

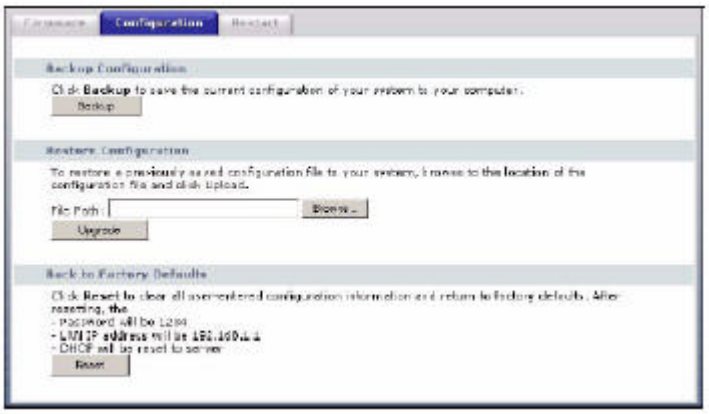
Figura 94 Mensaje de Error

15.2 Pantalla de Configuración

Consulte el capítulo sobre Mantenimiento de los Ficheros de Firmware y Configuración para transferir los ficheros de configuración utilizando comandos FTP/TFTP.

Pulse sobre el enlace **Herramientas** bajo las opciones de **Mantenimiento**, y seleccione la pestaña **Configuración**. La información relativa a los parámetros por defecto, backup de configuración y restauración de la configuración aparecen a continuación.

Figura 95 Configuración



15.2.1 Backup de configuración

El backup de la configuración permite guardar la configuración actual del P320W en un fichero de su ordenador. Una vez se disponga del P320W configurado y funcionando adecuadamente, es recomendable el hacer un backup del fichero de configuración antes de realizar cambios en el mismo. El fichero de backup es de gran utilidad en caso de necesitar volver a unos parámetros funcionales previos.

Pulse sobre **Backup** para guardar la configuración actual del P320W en su ordenador.

15.2.2 Restaurar configuración

El proceso de restauración de la configuración permite actualizar un fichero de configuración desde su ordenador a su P320W.

Tabla 62 Mantenimiento: Restauración de la configuración

ETIQUETA	DESCRIPCIÓN
Localización del fichero	Introduzca la localización del fichero que desea actualizar en este campo o pulse **Explorar…** para encontrarlo.
Explorar…	Pulse sobre el botón **Explorar…** para localizar el fichero que quiere cargar.
Actualizar	Pulse sobre **Actualizar** para comenzar el proceso. El proceso de actualización puede llevar unos dos minutos.

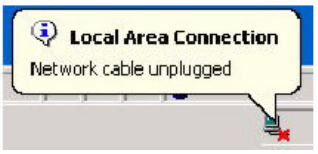
Nota: No apague el router mientras se actualiza el fichero de configuración en su equipo.

Tras ver la pantalla “Actualización Satisfactoria”, deberá esperar alrededor de un minuto antes de volver a acceder al equipo.

Figura 96 Restauración de la configuración

El P320W automáticamente se reinicia originando una desconexión de red temporal. En algunos sistemas operativos, podría ver el siguiente icono en su escritorio.

Figura 97 Desconexión temporal



Si ha actualizado el fichero de configuración por defecto será necesario que la dirección IP de su ordenador se encuentre dentro de la misma subred que la dirección IP del P320W (192.168.1.1).

Si la actualización no se realizó satisfactoriamente, le aparecerá la siguiente pantalla.

Figura 98 Error en la restauración de la configuración

15.2.3 Restauración de Parámetros por Defecto

Presionando el botón **Restaurar** dentro de esta sección se borran todos los parámetros de configuración introducidos por el usuario y se restauran en el P320W los parámetros por defecto.

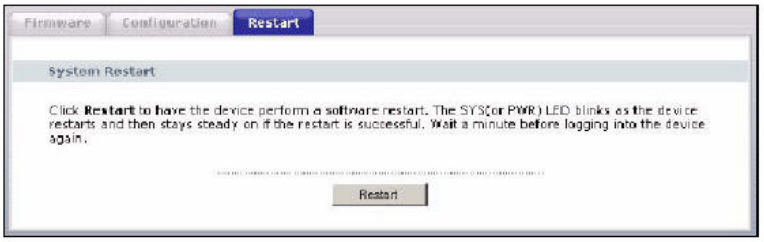
También es posible pulsar el botón **RESET** colocado en el panel posterior para restaurar los parámetros por defecto en su equipo. Consulte el capítulo 2 para obtener más información sobre el botón de Reset.

15.3 Pantalla de Reinicio

El reinicio del sistema permite reiniciar el P320W sin necesidad de desconectarlo de la alimentación.

Pulse sobre el enlace **Herramientas** bajo las opciones de **Mantenimiento**, y seleccione la pestaña **Reiniciar**. Pulse Reiniciar para reiniciar el equipo. Esto no afecta a la configuración del router.

Figura 99 Reinicio del Sistema



CAPÍTULO 16:TROUBLESHOOTING

Este capítulo cubre los potenciales problemas y sus respectivos remedios

16.1 Problemas en la fase de inicio

Tabla 63 Troubleshooting en la fase de inicio

PROBLEMA	ACCIÓN CORRECTIVA
No se ilumina ninguno de los LEDs del P320W	Asegúrese que el adaptador de corriente del equipo está correctamente conectado al gateway y a la toma de corriente. Verifique que la toma de corriente funciona correctamente. Compruebe que el switch de encendido del equipo está conectado. Si el error persiste, podría tratarse de un error hardware. En este caso, consulte con el distribuidor donde adquirió su equipo.

16.2 Problemas con la LAN

Tabla 64 Troubleshooting en LAN

PROBLEMA	ACCIÓN CORRECTIVA
Los LEDs de LAN no se iluminan	Compruebe las conexiones del cableado Ethernet. Asegúrese que los adaptadores de red de los equipos conectados funcionan correctamente.
No es posible acceder al P320W desde la LAN	Verifique que la dirección IP y la máscara de subred configurados en su ordenador se encuentran dentro de la misma subred que la configurada en el interfaz LAN del P320W.

16.3 Problemas con la WAN

Tabla 65 Troubleshooting en WAN

PROBLEMA	ACCIÓN CORRECTIVA
El LED WAN no se ilumina	Compruebe que las conexiones entre el puerto WAN del P320W y el equipo o medio de acceso a internet se encuentra correctamente realizado.
El interfaz WAN no obtiene dirección IP del ISP	Verifique los parámetros configurados en la interfaz WAN del P320W. El nombre de usuario y contraseña se aplican únicamente para la encapsulación PPPoE y PPTP. Asegure que tanto el Nombre de Usuario como la Contraseña tecleados son los correctos.

No existe conectividad con internet	Compruebe que el P320W está conectado y correctamente conectado. Verifique los parámetros de LAN. Asegure que el nombre de usuario y la contraseña se han tecleado correctamente.
La conexión con Internet se desconecta	Si está utilizando encapsulación PPPoE, marque la opción de "Conexión Forzada" para que la sesión PPP permanezca siempre levantada.

16.4 Problemas con la Contraseña

Tabla 66 Troubleshooting de Contraseña

PROBLEMA	ACCIÓN CORRECTIVA
No es posible el acceso al interfaz de configuración del P320W	El campo de contraseña distingue entre mayúsculas y minúsculas. Verifique que introduce la contraseña correcta con el tipo de letra adecuado. Utilice el botón de **RESET** para restaurar la configuración por defecto en el equipo. Esto hará que todos los parámetros del router vuelvan a sus valores de fábrica, incluida la contraseña (1234, por defecto)

16.5 Problemas con la Gestión Remota

Tabla 67 Troubleshooting de Gestión Remota

PROBLEMA	ACCIÓN CORRECTIVA
No es posible acceder al P320W ni desde LAN ni desde WAN	Consulte en la **sección 11.1** los casos en los que la gestión remota no es posible. Cuando el NAT está habilitado: • Utilice la dirección IP WAN del P320W cuando intente acceder desde el lado WAN • Utilice la dirección IP LAN del P320W cuando intente acceder desde el lado LAN

16.6 Problemas con el acceso al P320W

Tabla 68 Troubleshooting en el Acceso al P320W

PROBLEMA	ACCIÓN CORRECTIVA
El acceso al P320W no es posible	La contraseña por defecto es "1234". Este campo distingue entre mayúsculas y minúsculas. Por tanto, asegúrese que introduce la contraseña correctamente. Si ha modificado la contraseña de acceso y la ha olvidado, necesitará restaurar los parámetros por defecto en el equipo.
No es posible acceder al	Utilice la dirección WAN del P320W cuando lo esté configurando

configurador web	desde el lado WAN. Utilice la dirección LAN del P320W cuando lo esté configurando desde el lado LAN. Compruebe que tiene habilitado el servicio de gestión web (WWW). Si ha configurado una dirección IP de confianza, la dirección IP de su ordenador deberá coincidir con ésta. Consulte el capítulo de gestión remota para obtener más información. La dirección IP de su ordenador deberá estar dentro de la misma subred que la dirección IP configurada en el P320W. Asegure que los permisos para pop-ups, JavaScripts y Java están habilitados. Asimismo si ha desconectado el ordenador de otro dispositivo que está utilizando la misma dirección IP, entonces la tabla ARP del ordenador puede contener una entrada que mapea la dirección IP de gestión con la dirección MAC del dispositivo anterior. En Windows, utilice **arp –d** en la pantalla de símbolo del sistema para borrar las entradas de la tabla ARP.