cablemel

Guía rápida
Hitron CVE-30360

1. Introducción

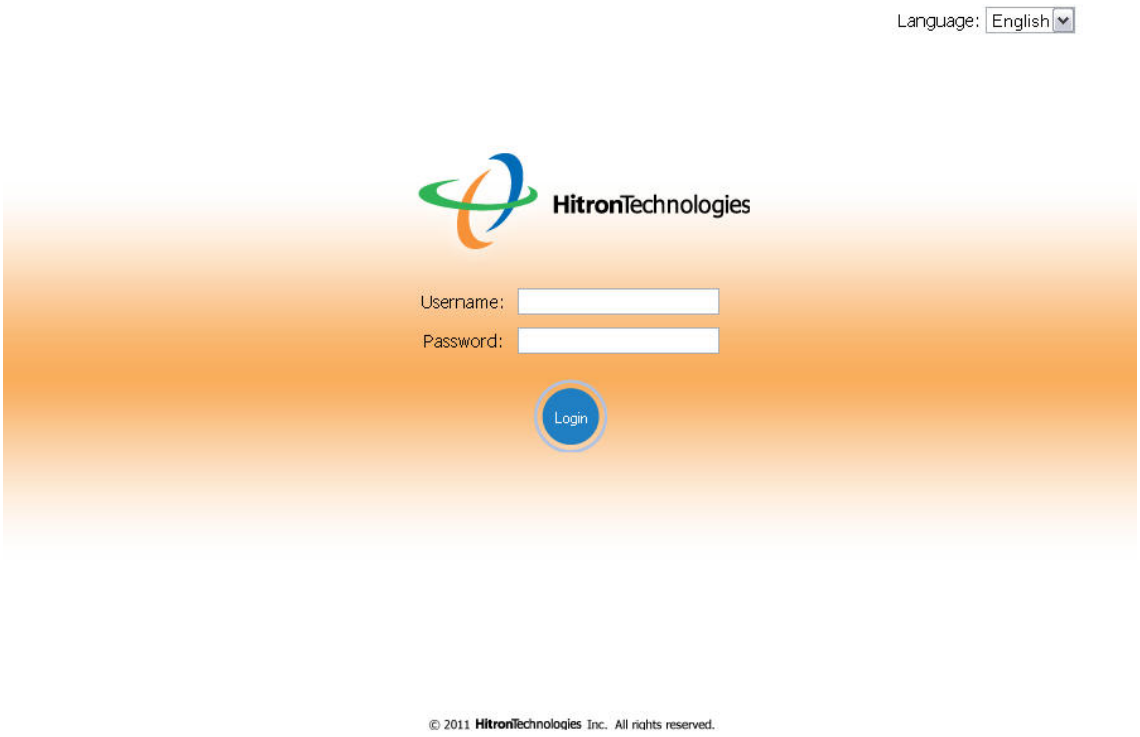
El nuevo cable módem router Hitron CVE-30360 introduce nuevas funcionalidades que hasta ahora ningún equipo doméstico era capaz de hacer. Esta guía pretende servir para configurar su enrutador y para describir estas nuevas funcionalidades de manera concisa pero clara.

2. Configuración de la conexión inalámbrica

El nuevo cable módem router Hitron CVE-30360, dispone de la última tecnología WIFI, por lo que si su dispositivo inalámbrico tiene una tarjeta WIFI 802.11n puede conectarse hasta a 300mbps.

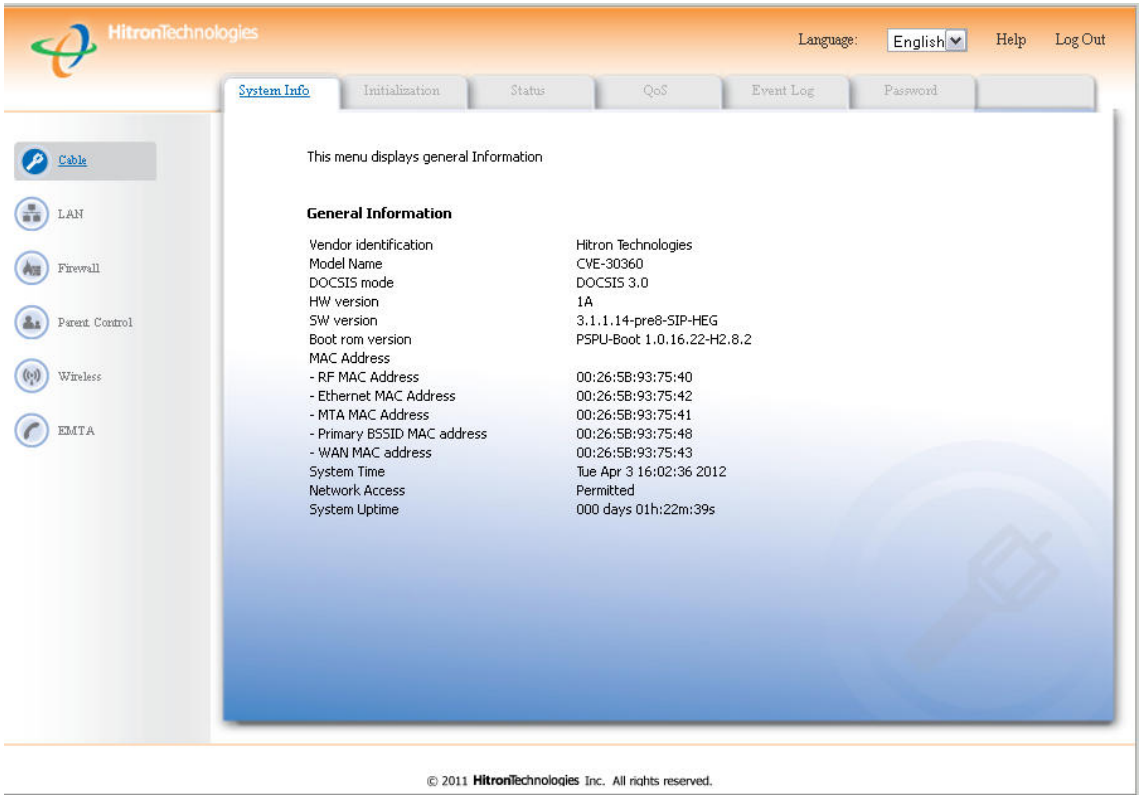
Para configurar su router, en primer lugar, debe abrir un navegador (Internet Explorer, Mozilla Firefox, Google Chrome, Opera, etc.) y en la barra de dirección poner http://192.168.0.1 o http://hitronhub.home

A continuación le saldrá una página donde se le solicita nombre de usuario y contraseña como ésta:

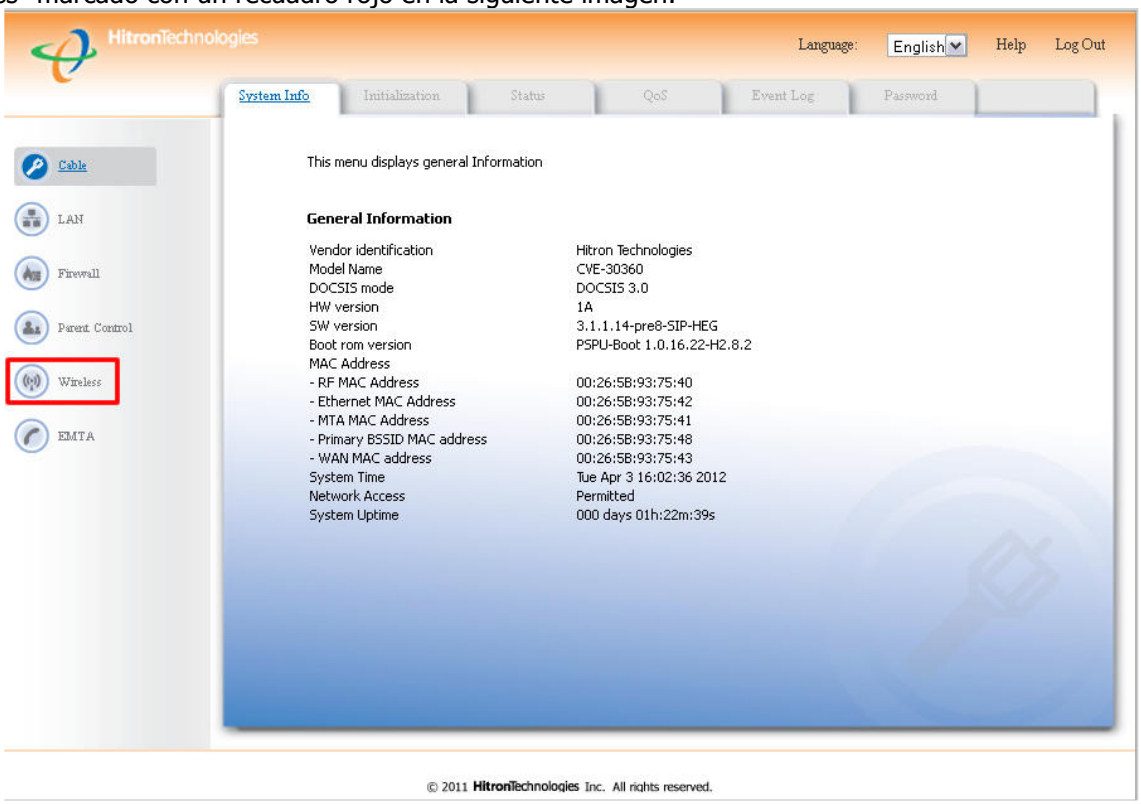


Las credenciales de acceso son:
Username: admin
Password: password

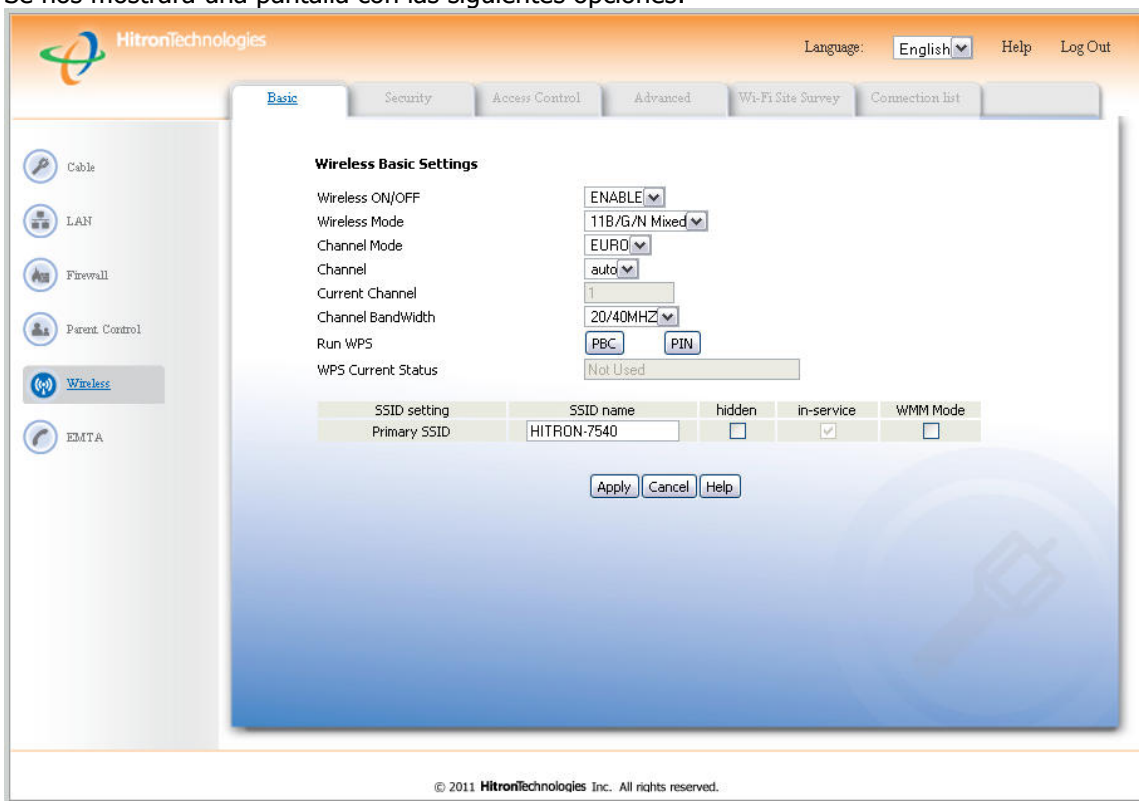
Una vez introducidas las credenciales, hacemos click en el botón redondo y azul con la palabra "Login" en el interior. Si hemos puesto los datos correctamente se nos mostrará una pantalla como la siguiente:



Para configurar nuestra conexión inalámbrica, debemos hacer click en el apartado "Wireless" marcado con un recuadro rojo en la siguiente imagen:



Se nos mostrará una pantalla con las siguientes opciones:

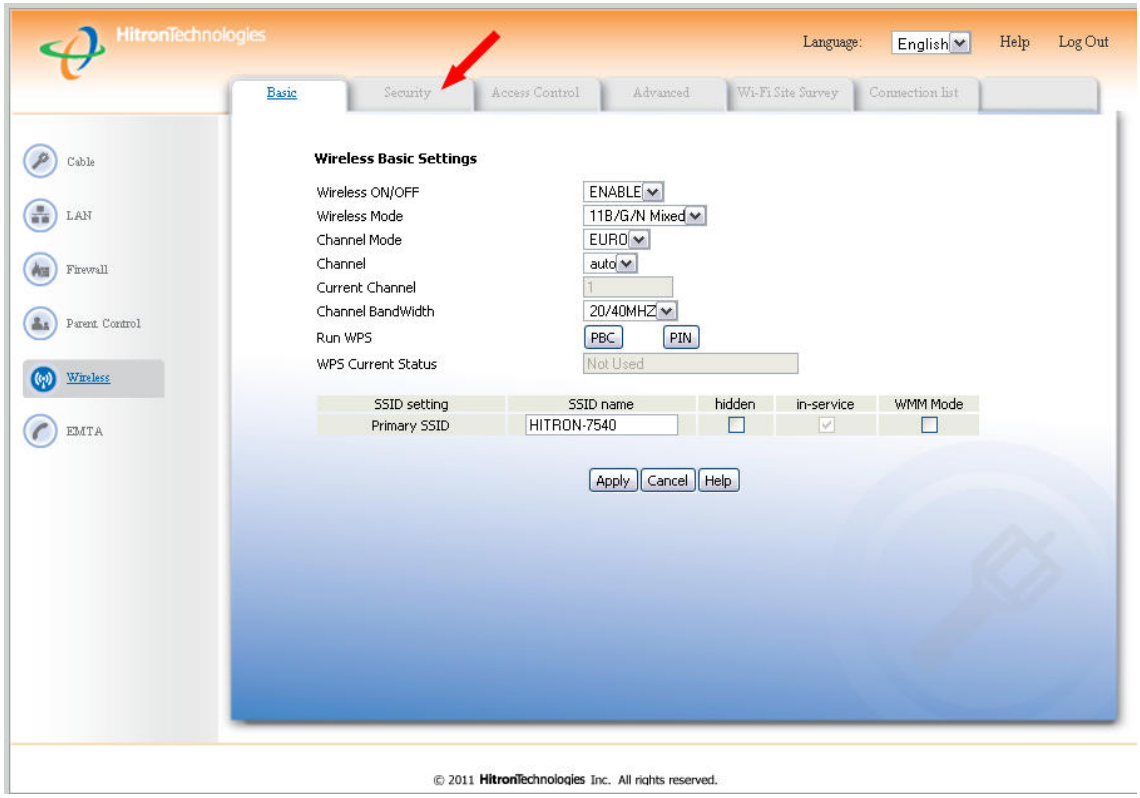


Intentaremos sintetizar qué es qué del siguiente menú. Por favor, si no conoce para que sirve alguna de las opciones, no la modifique, una configuración negligente puede derivar en un deterioro o en una pérdida de su conexión.

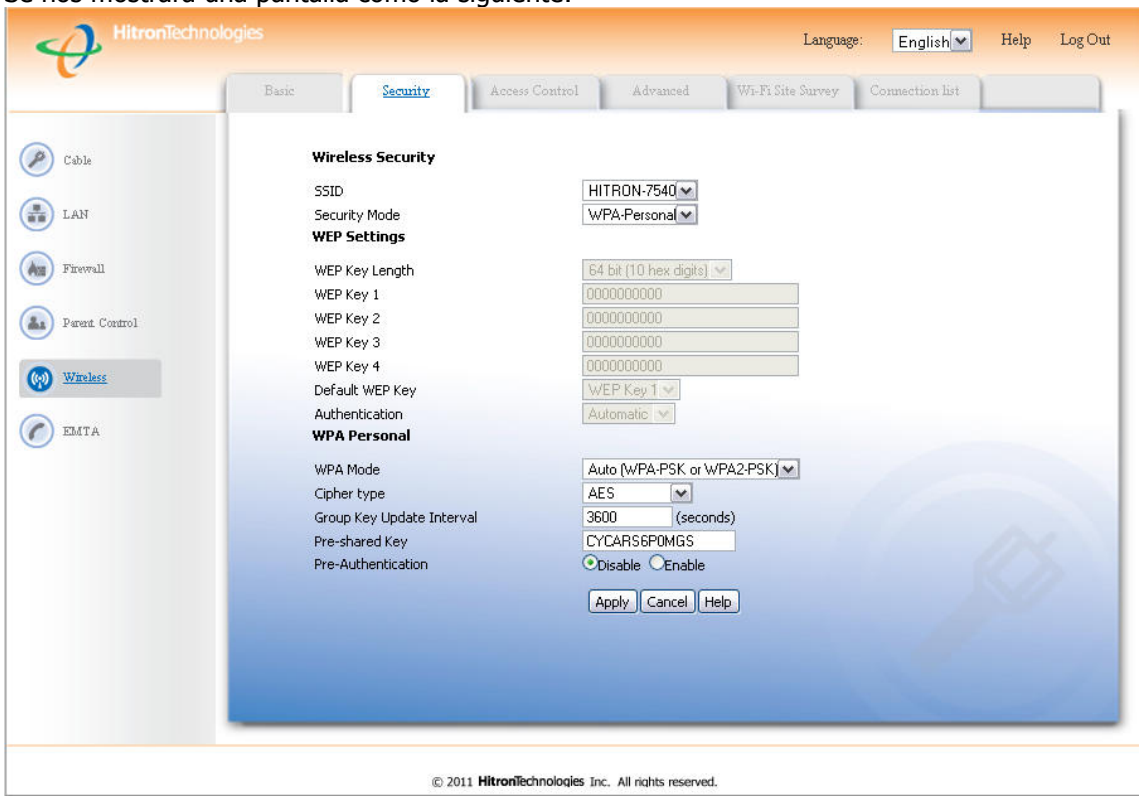
- Wireless ON/OFF: activa o desactiva el punto de acceso inalámbrico del router.
- Wireless Mode: tipo de conexión inalámbrica. El tipo B, es el tipo más antiguo de conexiones WIFI, sólo alcanza 11 mbps. El tipo G, es más actual que el B y puede llegar hasta a 54 mbps. El tipo N es el más actual de los protocolos WIFI, y puede llegar a 300 mbps. Si tiene dispositivos WIFI antiguos que son incapaces de conectarse, pruebe a cambiar esta opción. La opción por defecto no debe de generar ningún problema.
- Channel mode: esta opción debe estar en EURO.
- Channel: canal de emisión WIFI. Es recomendable que esté en "auto".
- Current Channel: canal de emisión en uso.
- Channel Bandwith: ancho de banda del canal. Es recomendable dejarlo en 20/40mhz
- Run WPS: el WPS es un standard que pretende automatizar la creación de una red WIFI segura mediante la creación de un PIN para conectarse a la misma. Se recomienda no usar, pues se han detectado vulnerabilidades.
- WPS Current Status: estado de WPS.
- En la última tabla aparece el nombre de nuestra red WIFI (SSID), si se encuentra oculta (hidden), si está operando (in-service) y el modo WMM (WIFI multimedia).

En conclusión, aquí debemos definir el nombre de nuestra red (SSID) en la tabla inferior y seleccionar "auto" en el canal y pulsar en el botón "Apply". Pasaremos ahora a configurar la seguridad.

Hacemos click en la pestaña "Security" marcada con la flecha roja en la siguiente imagen:



Se nos mostrará una pantalla como la siguiente:



Las opciones disponibles son:

- SSID: nombre de su red inalámbrica
- Modo de seguridad: las opciones son: **None**, sin ningún tipo de seguridad; **WEP**, encriptación débil, se recomienda no usar a no ser que su equipo inalámbrico no soporte WPA; **WPA-Personal**, el método de encriptación más seguro, se recomienda su uso.
- WEP Settings: opciones para la encriptación WEP, tal como longitud de la clave (cuanto más larga, más segura) y la posibilidad de definir hasta cuatro claves distintas.
- WPA Mode: posibilidad de elegir entre WPA, WPA2 (más segura) o Automático. Se recomienda para mayor compatibilidad dejar está opción en "Auto".
- Cipher type: tipo de cifrado. Posibilidad de elegir entre TKIP, AES o ambos simultáneos. AES es el cifrado más fuerte, pero es posible que no funcione con tarjetas WIFI antiguas. Si experimenta problemas, seleccionar la opción "TKIP and AES".
- Group Key Update Interval: intervalo de actualización. Se recomienda dejar en su opción por defecto, 3600.
- Pre-shared Key: clave que ha de introducir para conectarse a su red WIFI. Es obligatorio que contenga al menos ocho caracteres. Se pueden usar mayúsculas, minúsculas, números y caracteres especiales. Cuanto más compleja, más difícil será que la averigüen. Se recomienda anotarla en algún lugar seguro para no olvidarla.
- Pre-Authentication: esta opción se recomienda dejarla por defecto en "Disable".

3. Gestión del cortafuegos

La gestión de un cortafuegos es una tarea muy compleja, pues este elemento es el responsable de controlar los intentos de intrusión en los equipos que hay conectados al router, por lo que cualquier modificación ha de ser hecha sabiendo muy bien qué deseamos hacer, para sí no comprometer la seguridad.

Con este espíritu, tan sólo vamos a explicar en este apartado cómo abrir los puertos para un determinado programa, y como crear una DMZ para un equipo que necesita muchos puertos abiertos, como por ejemplo una consola de videojuegos.

3.1 Abrir un puerto o un rango de puertos

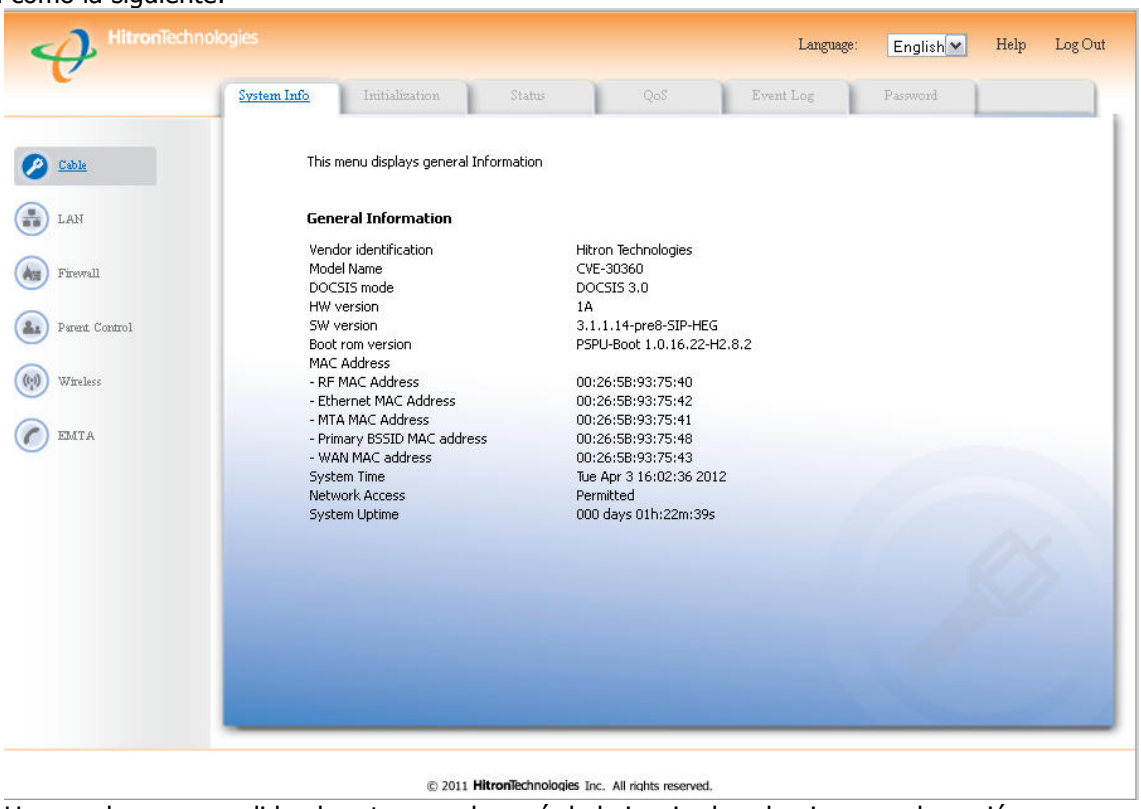
Si tenemos una aplicación instalada en nuestro ordenador que necesita tener un puerto o un rango de puertos, ya sea TCP o UDP abiertos (por favor, consulta la ayuda de tus aplicaciones para conocer este dato), vamos a pasar a explicar cómo realizar esta tarea.

En primer lugar debe abrir un navegador (Internet Explorer, Mozilla Firefox, Google Chrome, Opera, etc.) y en la barra de dirección poner http://192.168.0.1 o http://hitronhub.home

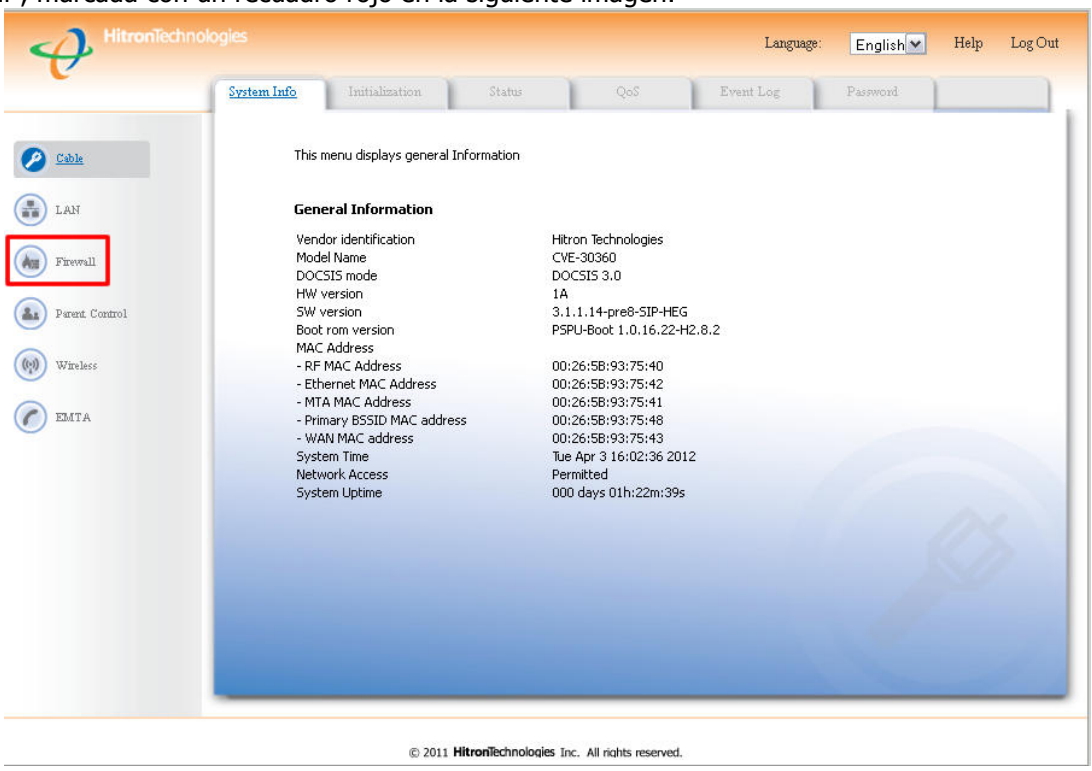
A continuación le saldrá una página donde se le solicita nombre de usuario y contraseña como ésta:

Las credenciales de acceso son:
Username: admin
Password: password

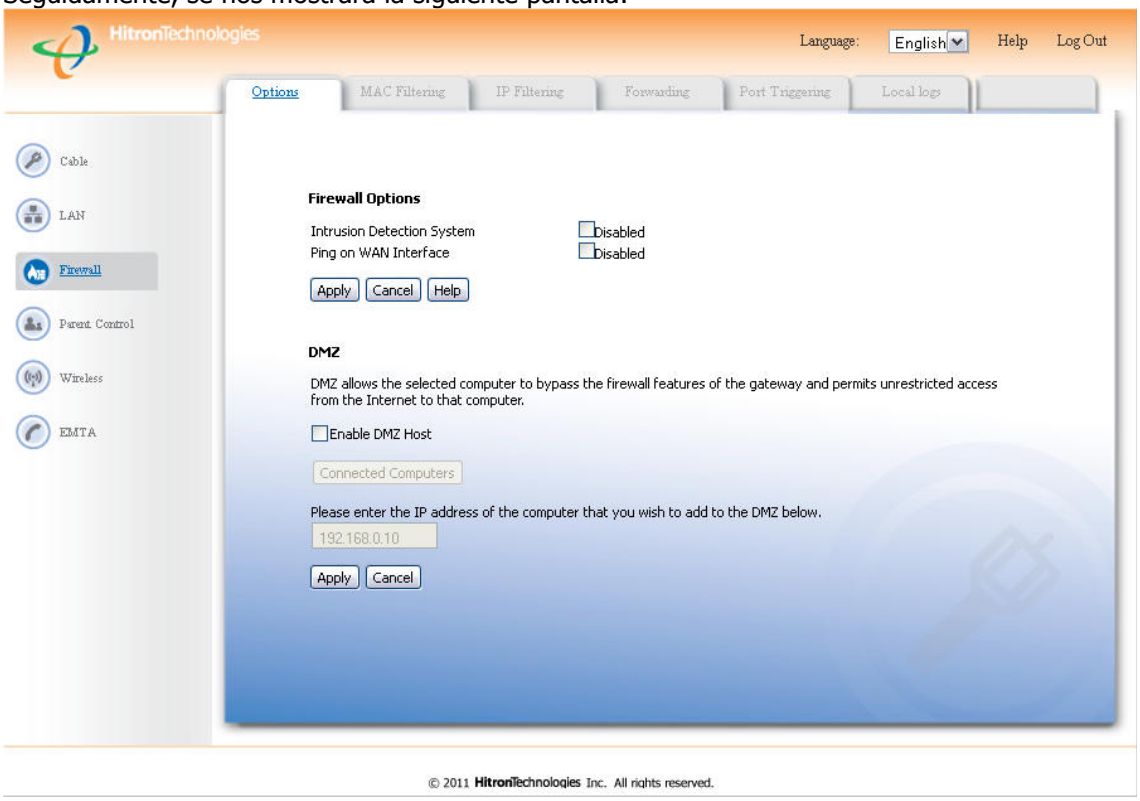
Una vez introducidas las credenciales, hacemos click en el botón redondo y azul con la palabra "Login" en el interior. Si hemos puesto los datos correctamente se nos mostrará una pantalla como la siguiente:



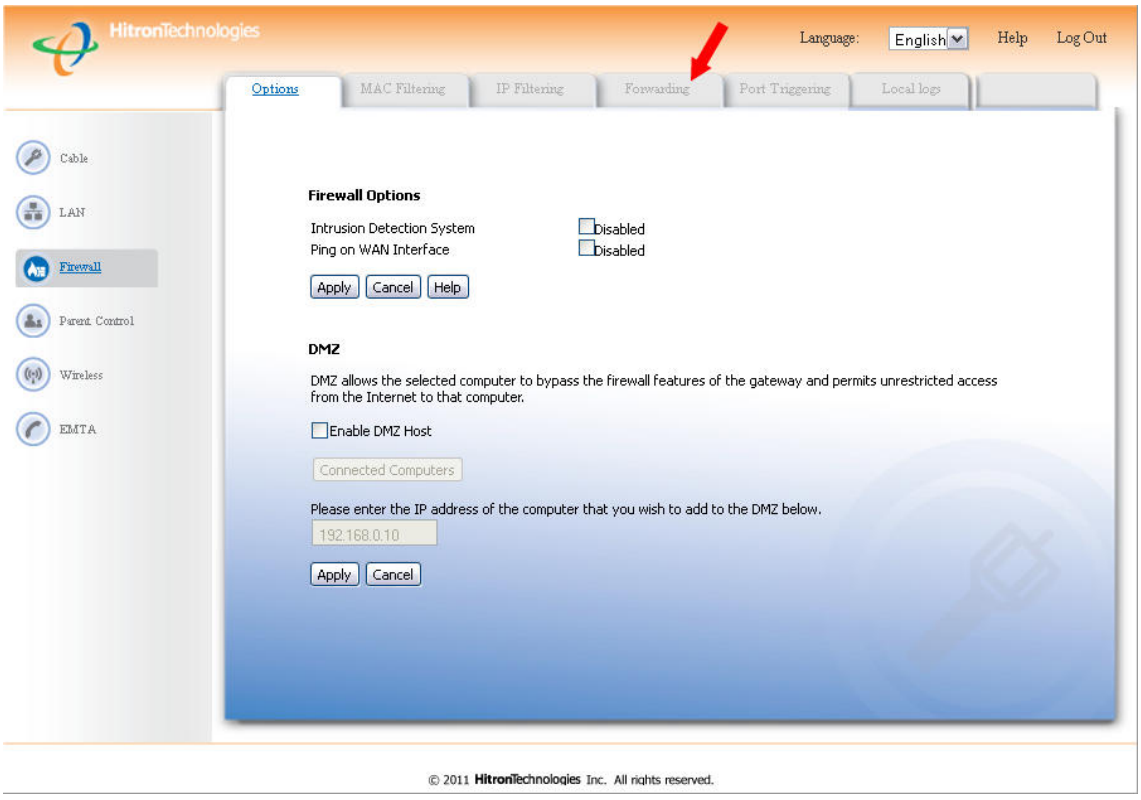
Una vez hemos accedido al router, en el menú de la izquierda seleccionamos la opción "Firewall", marcada con un recuadro rojo en la siguiente imagen:



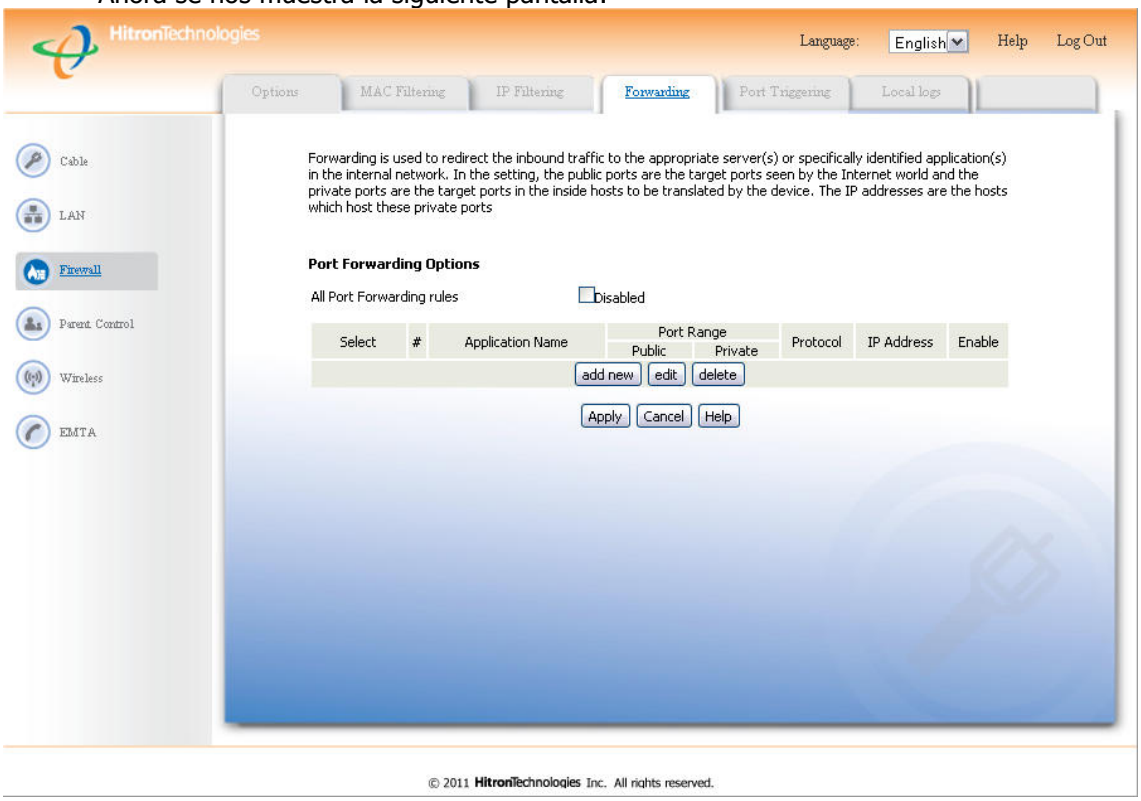
Seguidamente, se nos mostrará la siguiente pantalla:



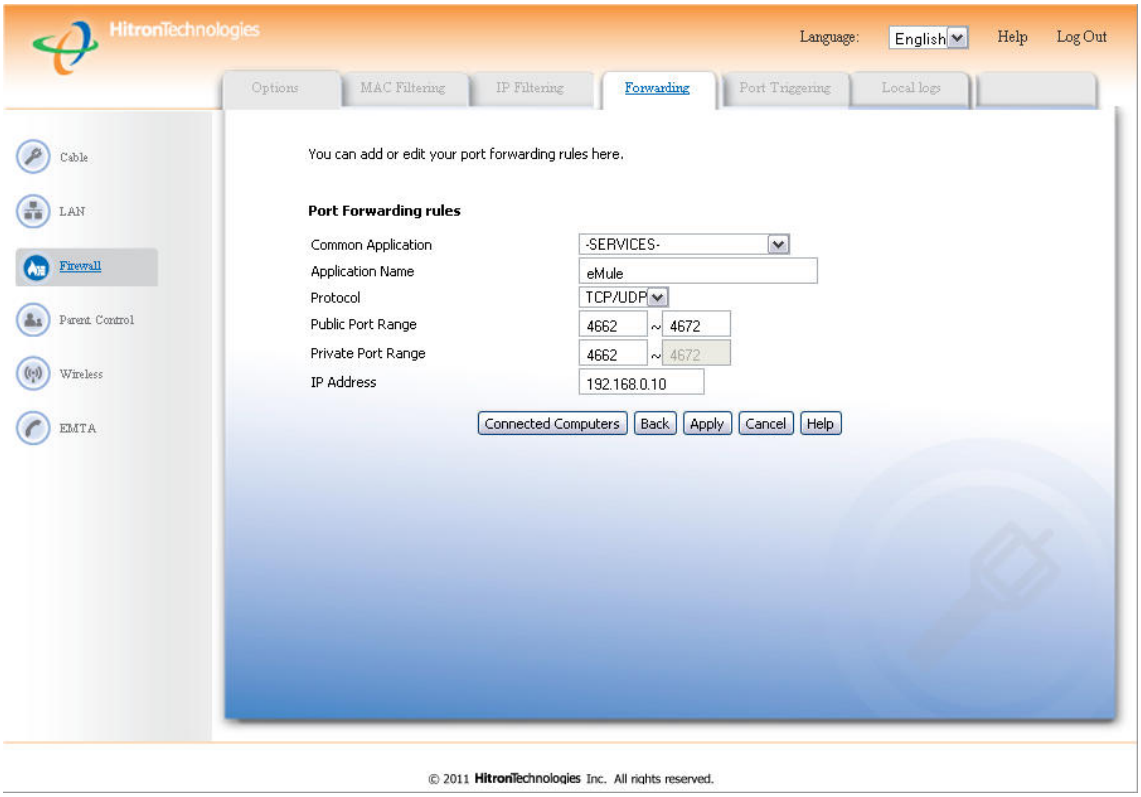
Hacemos click en la pestaña "Forwarding" marcada con una flecha roja en la siguiente imagen:



Ahora se nos muestra la siguiente pantalla:



Hacemos click en el botón "add new":



Pasamos a explicar brevemente cada una de las opciones:

- Common Application: En este desplegable se nos enumera una serie de aplicaciones conocidas, si seleccionamos una automáticamente se nos completarán los campos "Application Name", "Protocol" y "Public Port Range". Si nuestra aplicación no está en la lista, escogeremos la opción "-SERVICES-"
- Application Name: nombre de la aplicación, una simple etiqueta para reconocer el programa al que hemos abierto el o los puertos.
- Protocolo: podemos seleccionar según nuestras necesidades, TCP, UDP, TCP/UDP, GRE y ESP. Consultar la ayuda de la aplicación para saber el protocolo usado por la misma.
- Public Port Range: rango público de puertos. Rango de puertos que la aplicación necesita tener abiertos. Si tan sólo es un puerto, se rellenarán ambos campos con el mismo, si es un rango de puertos se pondrá en el primer campo el primer puerto del rango y en el segundo campo el último campo.
- Private Port Range: rango privado de puertos. Puertos configurados en el ordenador para el servicio configurado, normalmente se usan los mismos valores que en el "Public Port Range".
- IP Address: dirección IP del ordenador.

Una vez cumplimentados todos los campos pulsamos el botón "Apply" y se salvarán los datos.

3.2 Crear una DMZ

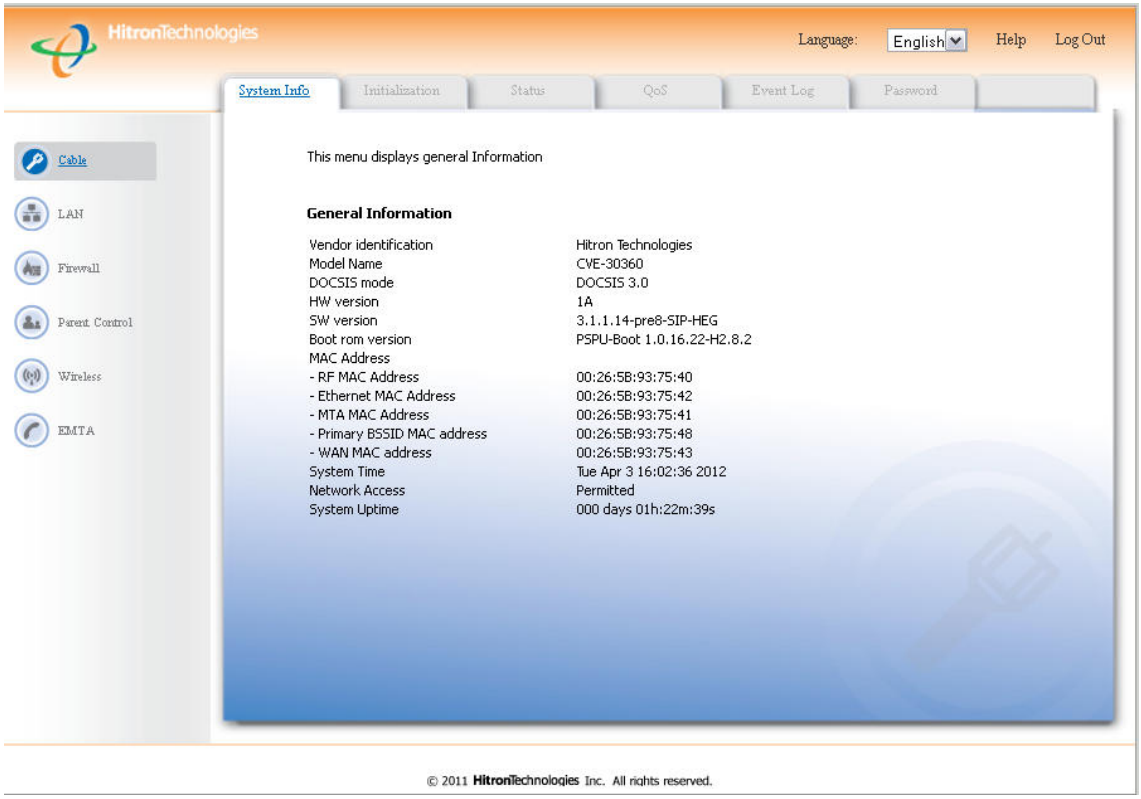
En seguridad informática, una zona desmilitarizada (DMZ, demilitarized zone) o red perimetral es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permitan a la red externa -- los equipos (hosts) en la DMZ no pueden conectar con la red interna. El motivo por el cual creamos una DMZ es para que un equipo no tenga ninguna limitación en cuanto a apertura de puertos. Un ejemplo de equipos ideales para estar en una DMZ son un segundo router o una consola de videojuegos. Es poco aconsejable poner un PC en una DMZ, pues será vulnerable a ataques e intentos de intrusión.

En primer lugar debe abrir un navegador (Internet Explorer, Mozilla Firefox, Google Chrome, Opera, etc.) y en la barra de dirección poner http://192.168.0.1 o http://hitronhub.home

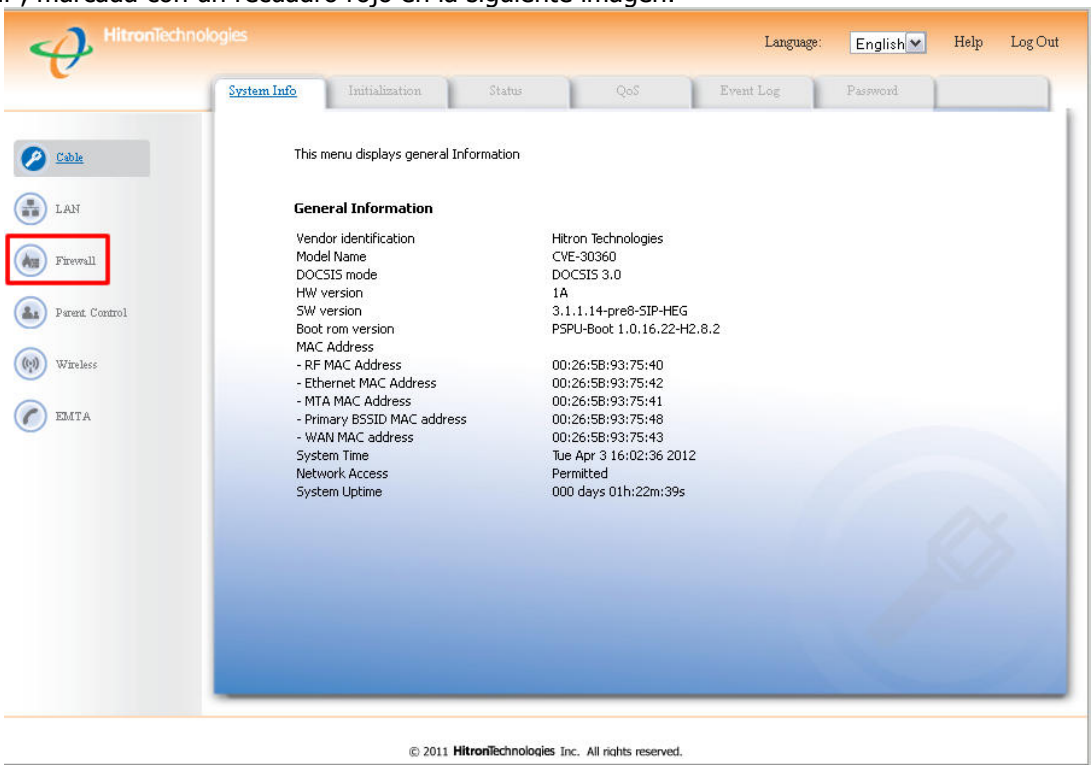
A continuación le saldrá una página donde se le solicita nombre de usuario y contraseña como ésta:

Las credenciales de acceso son:
Username: admin
Password: password

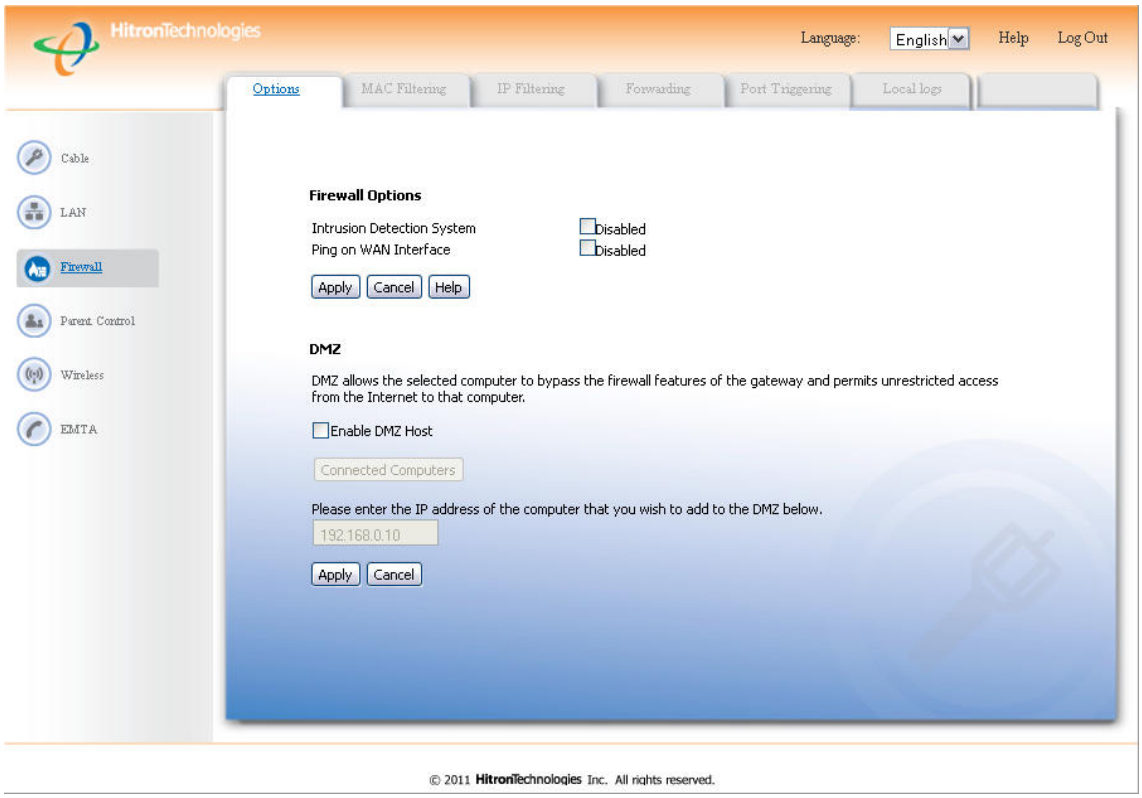
Una vez introducidas las credenciales, hacemos click en el botón redondo y azul con la palabra "Login" en el interior. Si hemos puesto los datos correctamente se nos mostrará una pantalla como la siguiente:



Una vez hemos accedido al router, en el menú de la izquierda seleccionamos la opción "Firewall", marcada con un recuadro rojo en la siguiente imagen:



Seguidamente, se nos mostrará la siguiente pantalla:



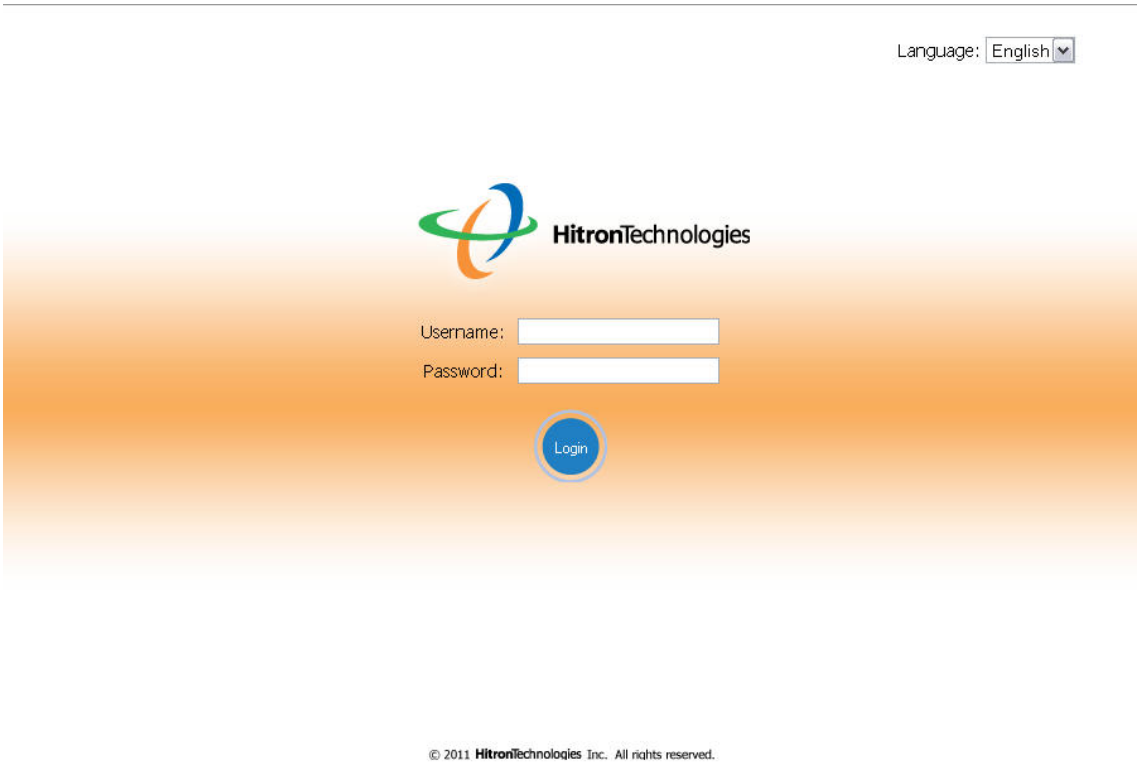
Aquí marcaremos la casilla "Enable DMZ Host" y en el campo bajo "Please enter the IP address of the computer that you wish to add to the DMZ bellow" pondremos la dirección IP del equipo que deseamos incluir en la DMZ. Tan sólo podemos incluir un equipo en la DMZ. Recomendamos que el equipo incluido en la DMZ no esté configurado con DHCP, si no que tenga fijada una IP del rango privado del router.

4 NAS (Disco duro en red)

Una de las novedades que presenta el nuevo router de Cablemel, es la capacidad de compartir con todos los usuarios de su red doméstica un disco duro o "lápiz" USB. El nuevo router Hitron tiene en su lateral derecho un puerto USB 2.0, al que se puede conectar una unidad de almacenamiento USB, al que podrá acceder desde cualquier ordenador de su casa.

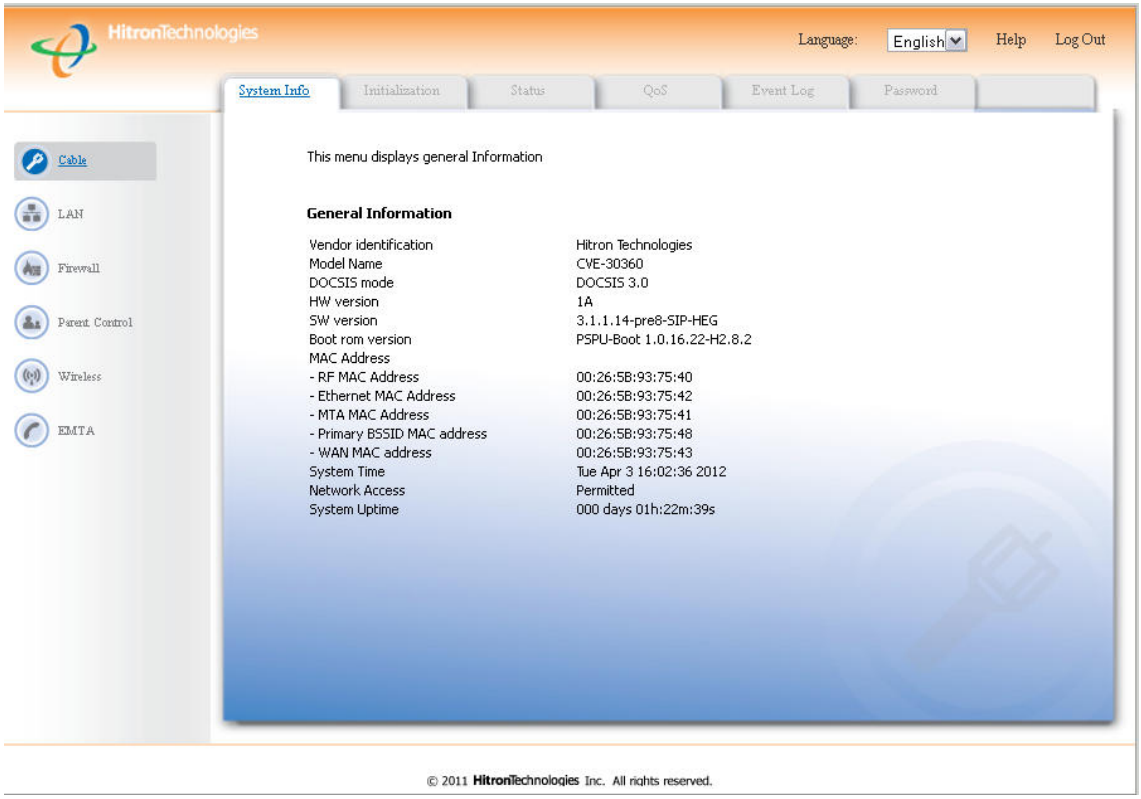
En primer lugar conectamos un disco duro o "lápiz" USB en el puerto del cable módem. Seguidamente, abrimos un navegador (Internet Explorer, Mozilla Firefox, Google Chrome, Opera, etc.) y en la barra de dirección poner http://192.168.0.1 o http://hitronhub.home

A continuación le saldrá una página donde se le solicita nombre de usuario y contraseña como ésta:

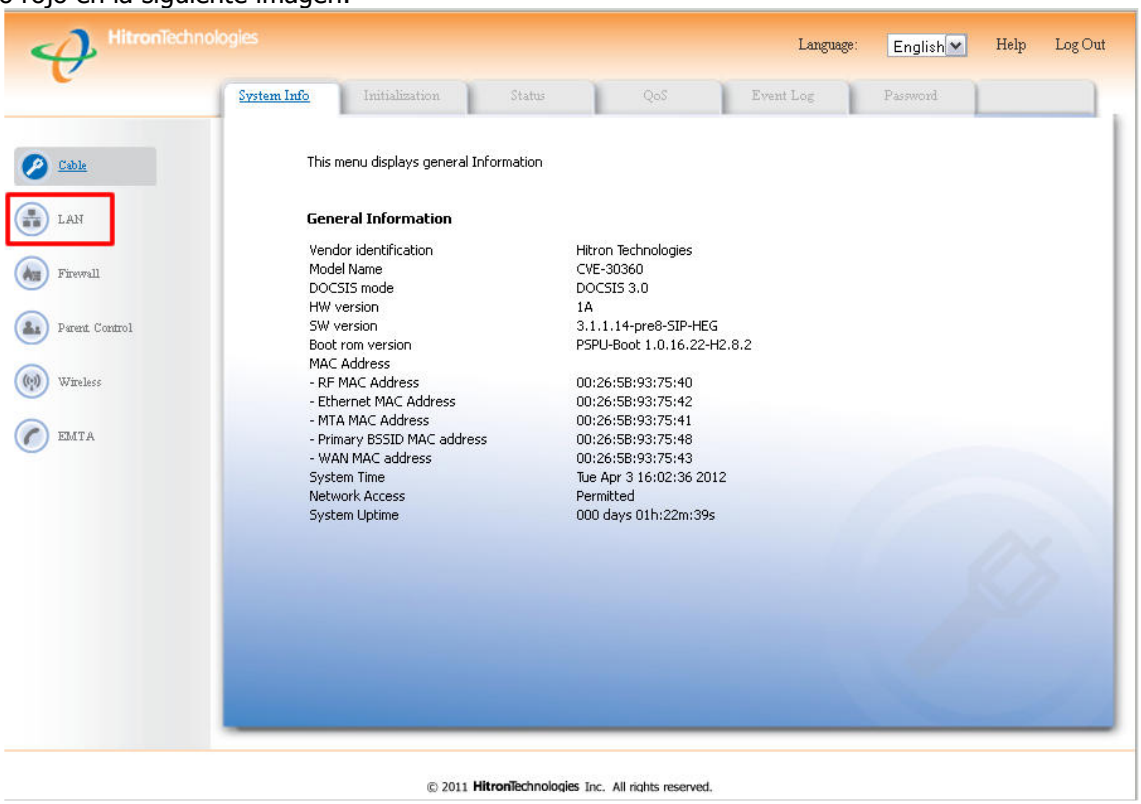


Las credenciales de acceso son:
Username: admin
Password: password

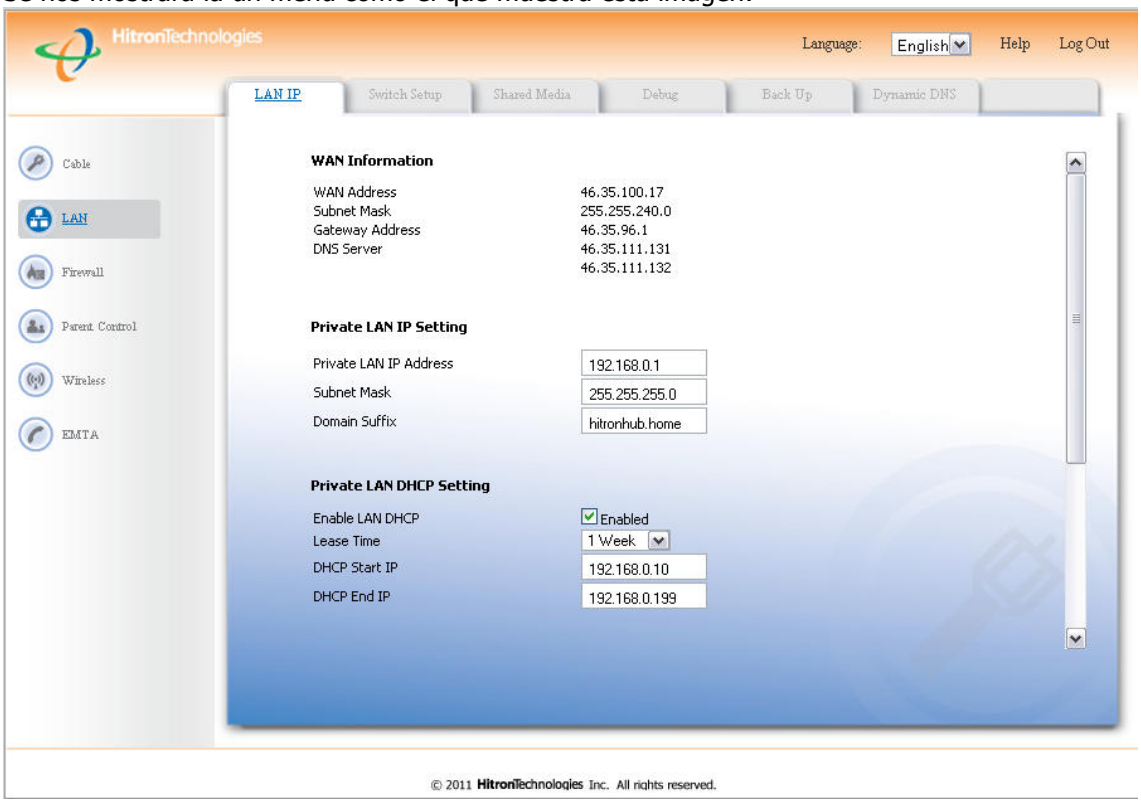
Una vez introducidas las credenciales, hacemos click en el botón redondo y azul con la palabra "Login" en el interior. Si hemos puesto los datos correctamente se nos mostrará una pantalla como la siguiente:



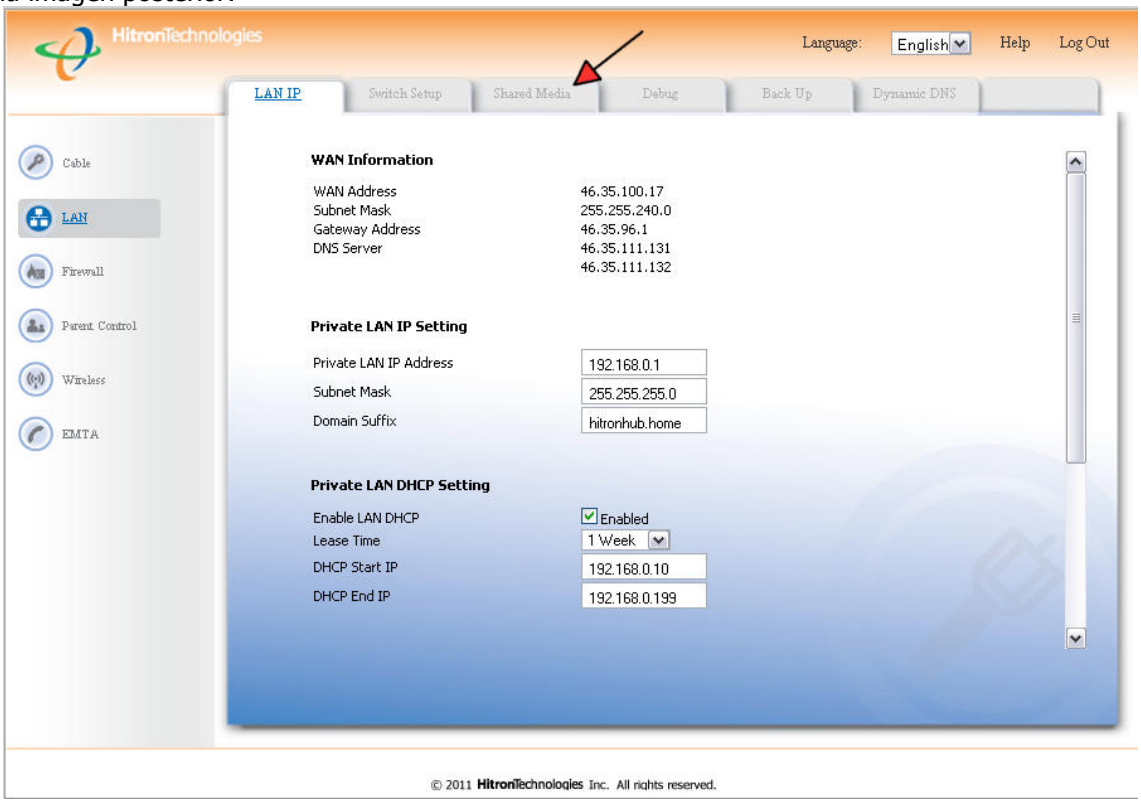
En esta pantalla, en la columna de la izquierda, hacemos click en "LAN", marcado en un recuadro rojo en la siguiente imagen:



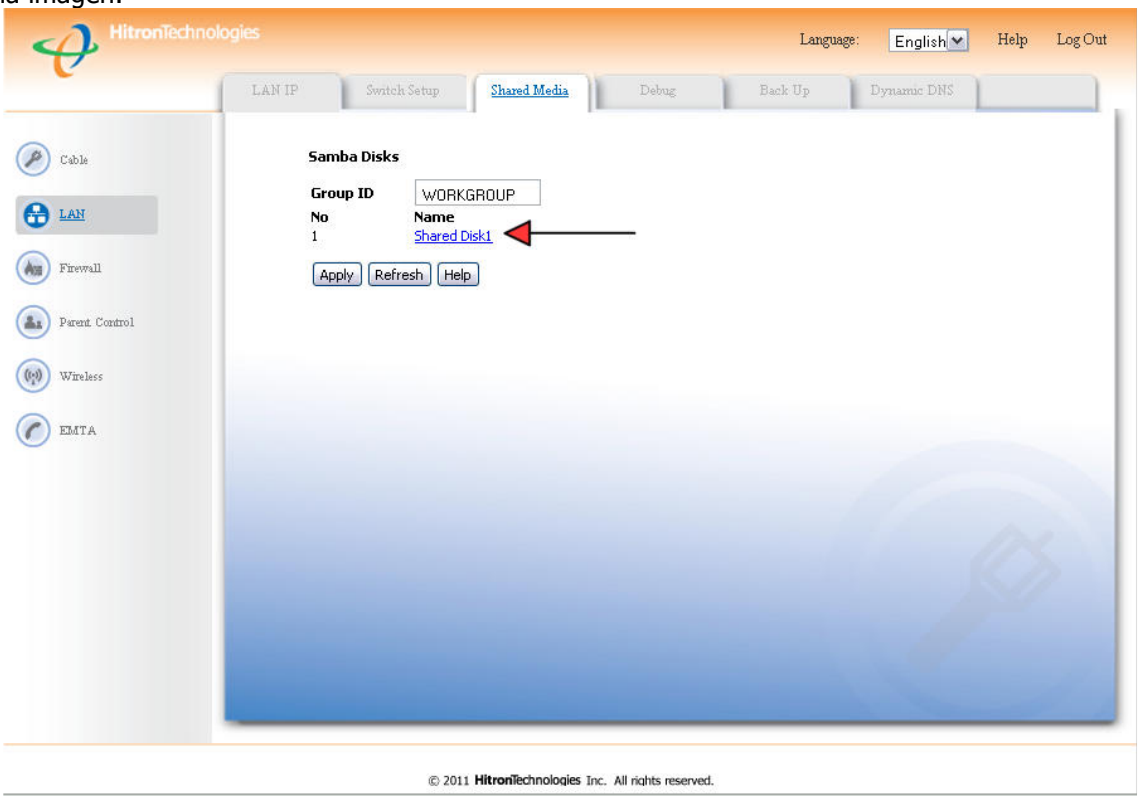
Se nos mostrará la un menú como el que muestra esta imagen:



En este menú, hacemos click en la pestaña "Shared Media", marcado con una flecha roja en la imagen posterior:



En la pantalla, si el cable módem ha reconocido satisfactoriamente la unidad de almacenamiento, le aparecerá "Shared Disk1" en el menú, tal y como se remarca con la flecha roja en la imagen:



Para acceder al disco compartido tan solo tiene que:

En Windows XP: Pulse el botón de "Inicio" ; Haga click en "Ejecutar"; Escriba \\192.168.0.1\Disk_sda1\ y haga click en el botón "Aceptar"

En Windows Vista\7: Pulse el botón de inicio en la barra de menú de Windows; escriba en el cuadro de diálogos que aparece \\192.168.0.1\Disk_sda1\ y pulse "enter".

En MacOS: En el "Finder" seleccione "Ir", "Conectarse al servidor"; en el campo "Dirección del servidor" escriba smb://192.168.0.1/Disk_sda1/

En este ejemplo hemos usado un disco con una sola partición, pero se puede usar discos con varias particiones, y todas serían compartidas como "Disk_sdax", donde la "x" es el número de la partición a la que queremos acceder. Por ejemplo, un disco con cuatro particiones tendría "Disk_sda1", "Disk_sda2", "Disk_sda3" y "Disk_sda4".

Anexo

SSID:_____

Contraseña:_____