

Equipo Integrado Fibra Óptica

TriWave

Manual de Fabricante



Índice

Índice	2
Introducción	6
Advertencias	7
Descripción del equipo	8
Características Técnicas	8
Diseño	
Vista Superior	
Vista Trasera	
Puesta en Marcha	
Interfaz de Usuario Web	
Parámetros por defecto	
Configuración IP	
Procedimiento de inicio de sesión	
Información de dispositivo	21
Device Info	21
WAN	22
Statistics	23
LAN	
WAN	
Route	25
ARP	26
DHCP	27
Configuración Avanzada	
Layer2 Interface	
GPON interface	
WAN Service	
LAN	
IPv6 AutoConfig	
NAT	
Virtual Servers	
Port Triggering	
DMZ Host	
Security	
IP Filtering Outgoing	
IP Filtering Incoming	40
Parental Control	42

Time Restriction	42
URL Filter	44
Quality of Service	46
QoS Queue	46
QoS Classification	
Routing	51
Default Gateway	51
Static Route	51
Policy Routing	52
RIP	54
DNS	55
DNS Server	55
Dynamic DNS	55
UPnP	57
DNS Proxy	
IP Tunnel	59
IPv6inIPv4	59
IPv4inIPv6	60
Multicast	61
Wireless	63
Basic	63
Security	66
MAC Filter	68
Wireless Bridge	69
Advanced	
Station Info	74
Voice	75
SIP Basic Setting	75
SIP Basic Setting	
SIP Advanced Setting	
Diagnostics	81
Management	82
Settings	82
Backup	82
Update	82
Restore Default	82
TR-069 Client	83
Internet Time	85

Access Control	
Passwords	86
Update Software	
Reboot	

Control de Versiones

Versión	Cambio realizado por	Descripción del cambio	Fecha
1.0		1ª Edición	30/09/2014

Introducción

Este manual proporciona información relativa al diseño, instalación y configuración del equipo TriWave y va dirigido a usuarios con conocimientos básicos de la terminología y conceptos en telecomunicaciones.

Si el equipo no funciona correctamente, puede contactar con el soporte técnico de Telnet Redes Inteligentes S.A. en la siguiente dirección de correo: <u>operaciones@telnet-ri.es</u>.

Para la descarga de nuevas actualizaciones, productos, manuales o actualizaciones de software, puede visitar nuestra página web: <u>http://www.telnet-ri.es</u>

Advertencias

El equipo TriWave está diseñado para su uso exclusivo en interiores. A continuación, se describen una serie de recomendaciones que debería tener en cuenta el usuario:

- Evita la humedad y acumulación de polvo.
- No instales este este producto cerca del agua. Por ejemplo, evitar instalaciones cerca de una bañera, lavadora,...
- Deja espacio a cada lado del equipo para la disipación de calor y no pongas objetos pesados sobre ella.
- No conectes la fuente de alimentación eléctrica en superficies elevadas. Evita conectarlas al aire libre. No se deben colocar objetos pesados sobre el cable eléctrico. Se debe evitar que el cable este en zona de tránsito para impedir pisar, caminar sobre él.
- Use únicamente la fuente de alimentación eléctrica suministrada con el equipo.
- En caso de tormenta de fuerte aparato eléctrico es recomendable la desconexión del cable de alimentación para evitar descargas.
- Desconecte siempre todos los cables y conexiones de corriente eléctrica antes de realizar un mantenimiento o reparación del producto.
- La conexión a la red de fibra óptica es sensible a torsiones, por lo que se recomienda no manipular dicho cable, ni conectarlo y desconectarlo sin indicación previa de un operador especializado.
- Dentro de la fibra viaja una señal óptica. Por favor, evita mirar el haz de luz que circula por la fibra pues puede dañar su visión. Evita manipular el cable sobre el que está adherida la etiqueta "Láser de clase 1".



PRODUCTO LASER CLASE 1 No mirar por la salida de la Fibra Óptica

Descripción del equipo

El equipo TriWave es un terminal diseñado para el uso en entornos de hogar y de negocio. Como equipo integrado de fibra óptica, tiene las propiedades de un equipo integrado, multipuerto y con capacidades inalámbricas que te permitirá la conexión de varios terminales de usuario a la línea FTTH de fibra óptica, basada en la tecnología GPON (Redes Ópticas Pasivas de Alta Capacidad), que proporciona canales de datos de alta velocidad.

Este equipo permite el acceso a la red IP, proporcionando servicios de alta calidad como la conexión a Internet, el servicio telefónico de Voz sobre IP, y el servicio de TV por Internet sin necesidad de ningún equipo adicional.

Características Técnicas

Características Hardware

• 1 puerto óptico SC/APC con acceso GPON (ITU-T G.984.x)

Interfaz G.984.2	Transmisión		Recepción		
	Longitud de onda	Potencia de Transmisión	Longitud de onda	Sensibili dad	Potencia Saturación
B+	1260-1360nm	+0,5/ +5 dBm	1480-1500nm	-28 dBm	> -8 dBm
C+	1290-1320nm	+0,5/ +5 dBm	1480-1500nm	-30 dBm	> -8 dBm

- 3 puertos LAN RJ45 IEEE 802.3ab 10/100/1000 Base-T
- 1 puertos de telefonía RJ11 (Interfaz POTs: G.711 A/u, T.38, RTP/RTCP, SIP). Interfaces FXS

Interfaz FXS (RJ11). Puertos Telf 1-2. Características de transmisión	Valores
Nivel de la señal portadora a la salida	-16 dBm
Banda de frecuencias	300-3400 Hz
Frecuencia de referencia de niveles relativos	1020 Hz
Impedancia nominal	600 Ohms resistivos
Nivel de ruido	< -60dBm
Nivel medio máximo de TX (entrada PTR)	< -10dBm (10s)
Nivel de pico máximo	< 1,5V

• Punto de acceso WIFI 802.11b/g/n con dos antenas de 3dBi (IEEE802.11n, compatible con clientes IEEE802.11b/g. Autenticación: IEEE 802.1x, a través EAP. Seguridad: IEEE 802.11i/e)

Funcionalidades LAN

- 3 puertos 10/100/1000BaseT Ethernet RJ-45 IEEE 802.3
- Autodetección de cable ethernet cruzado (Auto-MDI/MDI-X)
- Implementación bridge IEEE 802.1d
- Configuración de VLANs según el estándar 802.1Q
- Priorización de tráfico a nivel 2 mediante 802.1p
- Servidor DHCP

Características Wifi

- Punto de acceso IEEE 802.11b/g/n
- Soporte WEP, WPA, WPA2
- Soporte WPS/WPS 2.0

Routing

- Encapsulación IPoE según RFC2684 (evolución de la RFC 1483)
- Encapsulación PPPoE según RFC 2516
- Soporte de protocolo RIP v1 y v2
- IP multicast, IGMP snooping, IGMP proxy
- ICMP según RFC 1256
- NAT/PAT
- Soporte FullCone NAT
- DHCP client/relay
- DNS proxy
- Calidad de Servicio:
- Clasificación de tráfico por puerto, dirección IP, protocolo IP, 802.1p, DSCP o rango de puertos TCP/UDP
- Hasta 8 colas de salida
- Gestión de colas mediante WRR o SP
- Traffic shaping

Capacidades Firewall

- Filtrado por dirección origen, dirección destino, puerto origen y puerto destino
- Stateful Packet Inspection
- Redirección de puertos

Telefonía

- Cliente VoIP
- Ofrece dos puertos FXS
- Provisión mediante OMCI o TR-104

Gestión

- Gestión mediante interfaz web
- Gestión remota mediante TR-069
- Provisión de canal GPON mediante OMCI
- FTP o HTTP para descargas de configuración y actualización de software

Alimentación y Normativas

- Alimentación 12VDC-2,5A. ETSI ES 202 874-1 V1.2.1 (2012-05).
- Condiciones Ambientales: ETSI 300 019 –1-1/1-2/1-3.
- Resistencia: EN 60068-2-31:2008/-2-32
- Compatibilidad Electromagnética: EN 300 328 V1.7.1 (2006-10); EN 301-489-1 V1.8.1 + EN 301-489-17 V2.1.1
- Emisiones: EN 50385: 2002. Seguridad e Inmunidad: EN 60950-1:2006 + A11:2009 + A1:2010 + A12:2011; EN 62311 (2008-11); IEC 60825-1

Diseño

Vista Superior



Indicador	Estado Actual	Significado	
Power	Verde fijo	El "Equipo Integrado Fibra Óptica" está alimentado.	
	Verde intermitente (lento)	El "Equipo Integrado Fibra Óptica" está arrancando.	
	Rojo fijo (20 segundos)	Fallo en el equipo durante el Post (Power On Self Test).	
	Rojo intermitente (lento)	Fallo en el equipo durante el Post (Power On Self Test).	
	Apagado	El "Equipo Integrado Fibra Óptica" no está encendido.	
Eth 1-3	Verde fijo	Dispositivo conectado al puerto Ethernet. Enlace Ethernet	
		establecido.	
	Verde intermitente (lento)	Tráfico de datos en el puerto Ethernet.	
	Apagado	No hay dispositivo conectado en puerto Ethernet.	
Telf 1	Verde fijo	Servicio de voz disponible	
	Verde intermitente (lento)	En proceso de registro con la red.	
	Rojo fijo	Fallo de registro con la red.	
	Apagado	No se dispone del servicio VoIP. No provisionado.	
Wifi	Verde fijo	Interfaz Wifi habilitado.	
	Verde intermitente (lento)	Hay tráfico de datos en la interfaz Wifi.	
	Apagado	Interfaz Wifi deshabilitado.	

WPS	Verde fijo (120 segundos)	Ventana WPS activa	
	Rojo fijo	Problemas WPS.	
	Apagado	WPS habilitado pero ventana WPS inactiva.	
Internet	Verde fijo	Hay conexión PPPoE.	
	Verde Intermitente (lento)	Negociación sesión PPPoE.	
	Verde Intermitente (rápido)	Hay tráfico de datos.	
	Rojo fijo	Fallo en la autenticación.	
	Apagado	No hay conexión a Internet.	
Conexión	Verde fijo	Enlace fibra óptica establecido. PON sincronizada.	
	Apagado	Enlace de fibra óptica no establecida. PON no sincronizada	
Alarma	Rojo fijo	Nivel de potencia de señal óptica no adecuado	
	Apagado	Nivel de señal óptica adecuado	

Vista Trasera



Conector	Descripción
12V-2.5A	Conector de cable de alimentación de corriente.
On/ Off	Pulsando interruptor se enciende/ apaga el equipo.
Fibra Óptica	Conector Fibra Óptica SC/APC.
Telf 1	Puerto RJ11 que permite conectar terminales telefónicos.
Eth 1-3	Conector hembra RJ45. Switch de conectores para LAN.
Wifi/ WPS	Activación / Desactivación de Wifi con pulsación corta. WPS con pulsación larga.
Reset	Con pulsación corta, reinicio TV MOVISTAR. Con pulsación larga, se restablece la configuración de fábrica.

Puesta en Marcha

En las siguientes figuras le indicamos la conexión entre el equipo TriWave y los dispositivos asociados.

- El cable de alimentación se conecta al conector macho de alimentación del equipo indicado con 12V-2.5A
- El cable de fibra óptica se conecta en el conector correspondiente durante la instalación del servicio de Fibra Óptica.
- El botón de la parte trasera ha de estar en posición de encendido (ON).

<u>Nota</u>: La puesta en marcha será realizada por un operador especializado, por lo que se recomienda se manipule lo menos posible a este equipo. Para cualquier incidencia o duda con el funcionamiento del equipo, contacta con el servicio

técnico a través de los números de atención al cliente.

<u>Nota</u>: Debes tener en cuenta que para que el equipo esté completamente operativo, el indicador luminoso "Conexión" debe estar encendido en verde fijo. Este indicador en verde muestra que la conexión se ha realizado de manera correcta y se ha llevado a cabo la identificación y registro del dispositivo en la plataforma óptica.

- Se deberá introducir el ONU ID para que el equipo integrado de fibra óptica, TriWave se registre en la plataforma de fibra óptica. Operación a realizar por el instalador a través del portal web de Instalación y Mantenimiento (uso restringido a personal cualificado).
- Conexión de terminales según servicios (datos/ IPTV, teléfono, TV).



Fig. A

Fig. B





- Fig. A. Conexión TriWave a roseta fibra óptica.
- Fig. B. Conexión TriWave a equipos de usuario a través de conexión Ethernet (servicios datos/ IPTV/ VoIP).
- Fig. C. Conexión TriWave a teléfono (servicio de voz).

Interfaz de Usuario Web

Este apartado describe cómo acceder al dispositivo mediante el interfaz web. Exploradores compatibles: Internet Explorer 9.0+, Chrome, Firefox,... (Ver *"Guía de Navegadores.pdf*").

Parámetros por defecto

Los parámetros de fábrica del dispositivo son:

Parámetro	Valor
Dirección IP LAN	192.168.1.1
Máscara de subred LAN	255.255.255.0
Acceso administrativo	Usuario: 1234, Contraseña: 1234
Acceso usuario	Usuario: 1234, Contraseña: 1234
Dirección IP en la WAN	Ninguna
Acceso remoto vía WAN	Desactivado
Punto de acceso inalámbrico (Wifi)	Activado
Nombre de red inalámbrica o	Ejemplo: MOVISTAR_XXXX
Service Set IDentifier (SSID)	

Configuración IP

MODO DHCP

Una vez el equipo TriWave esté encendido y en funcionamiento, el servidor DHCP estará activo. El servidor DHCP, asigna direcciones IP a los dispositivos conectados a la LAN.

Para obtener una dirección IP del servidor DHCP, se deben seguir los siguientes pasos:

<u>Nota</u>: Se indican los pasos a seguir en un ordenador con sistema operativo Windows XP. Los pasos a seguir en la mayoría de los sistemas operativos son similares. En caso de duda, consulte la documentación de su sistema operativo y el documento "Guía de Navegadores.pdf".

Paso 1: Desde la ventana de "Conexiones de Red", abra la conexión de área local. También se puede acceder a esta ventana haciendo doble clic en el icono de conexiones de área local de la barra de tareas. Haga clic en el botón "Propiedades".

Paso 2: Seleccione Protocolo Internet (TCP/IP) y haga clic en el botón "Propiedades".

Paso 3: Seleccione "Obtener una IP automáticamente" como se muestra a continuación.

Propiedad	les de Protocolo Internet (TCP/IP)	? 🔀	
General	Configuración alternativa		
Puede l red es c con el a	Puede hacer que la configuración IP se asigne automáticamente si su red es compatible con este recurso. De lo contrario, necesita consultar con el administrador de la red cuál es la configuración IP apropiada.		
<u>⊙ 0</u> t	otener una dirección IP automáticamente		
- O U <u>s</u>	sar la siguiente dirección IP:		
<u>D</u> irec	ción IP:		
Máso	cara de subred:		
Puer	ta de enlace predeterminada:		
00	ptener la dirección del servidor DNS automáticamente		
<u>−O U</u> :	sar las siguientes direcciones de servidor DNS:		
Serv	idor DNS preferido:		
Serv	idor DNS alternati <u>v</u> o:		
	Opciones <u>a</u> vanzad	as	
	Aceptar	ancelar	

Paso 4: Haga clic en el botón "OK" para aplicar los cambios.

Si encuentra dificultades al usar el modo DHCP, puede configurar el modo de direccionamiento IP estático.

MODO DE DIRECCIONAMIENTO DE IP ESTÁTICO

En este modo de funcionamiento, el direccionamiento IP del dispositivo no es asignado automáticamente por el equipo TriWave, sino que se establece directamente en el dispositivo terminal de usuario. Para ello, debe seguir las siguientes instrucciones.

<u>Nota</u>: Se indican los pasos a seguir en un ordenador con sistema operativo Windows XP. Los pasos a seguir en la mayoría de los sistemas operativos son similares. En caso de duda, consulte la documentación de su sistema operativo y el documento "Guía de Navegadores.pdf".

Paso 1: Desde la ventana de "Conexiones de Red", abra la conexión de área local (también se puede acceder a esta ventana hacienda pulsando doble clic en el icono de conexiones de área local de la barra de tareas).
Haga clic en el botón "Propiedades"

Paso 2: Seleccione Protocolo Internet (TCP/IP) y haga clic en el botón "Propiedades".

Paso 3: Cambie la dirección IP a una IP dentro del rango 192.168.1.x (2<x<255) con máscara de subred 255.255.255.0 y puerta de enlace: 192.168.1.1 como se muestra a continuación:

Propiedades de Protocolo Internet (ТСРЛР) 🛛 🥐 🔀		
General		
Puede hacer que la configuración IP se red es compatible con este recurso. De con el administrador de la red cuál es la	e asigne automáticamente si su lo contrario, necesita consultar a configuración IP apropiada.	
O <u>D</u> btener una dirección IP automát	icamente	
💿 U <u>s</u> ar la siguiente dirección IP: —		
Dirección IP:	192.168.1.234	
<u>M</u> áscara de subred:	255 . 255 . 255 . 0	
Puerta de enlace predeterminada:	192.168.1.1	
O Obtener la dirección del servidor D	DNS automáticamente	
─⊙ Usar las siguientes direcciones de	servidor DNS:	
Se <u>r</u> vidor DNS preferido:		
Servidor DNS alternati <u>v</u> o:	· · ·	
	Opciones <u>a</u> vanzadas	
	Aceptar Cancelar	

Paso 4: Haga clic en el botón "OK" para aplicar los cambios.

Procedimiento de inicio de sesión

Para acceder a la interfaz de usuario web, debe realizar los siguientes pasos:

Paso 1: Inicie el navegador de Internet e introduzca la dirección IP del dispositivo en la barra de direcciones web. Por ejemplo: <u>http://192.168.1.1:8080</u>.

<u>Nota</u>: Para administración LOCAL (por ejemplo acceso LAN), el PC que ejecuta el navegador de Internet debe estar conectado al Puerto Ethernet del equipo TriWave.

Paso 2: El siguiente cuadro de diálogo aparecerá, como se indica a continuación. Introduzca el nombre de usuario y contraseña (user: 1234/ password: 1234)

Conectarse a 192.1	68.1.18	? 🔀
		G P
El servidor 192.168 nombre de usuario Advertencia: este s de usuario y contra (autenticación bási	3.1.18 en Broadband Ro y una contraseña. servidor está solicitando iseña se envíen de forn ca sin conexión segura)	outer requiere un o que su nombre na no segura).
<u>U</u> suario:	1	~
<u>C</u> ontraseña:		
	<u>R</u> ecordar contras	eña
	Aceptar	Cancelar

Haga clic en el botón "OK" para continuar

Nota: La contraseña de acceso puede ser cambiada posteriormente (ver apartado 8.5.1)

Paso 3: Después de acceder satisfactoriamente la primera vez, se le mostrará la siguiente pantalla.

🗋 Fiber Home Gateway 🛛 🗙							
	.92.168.1.1:8080/m	ain.html					
Movistar	Device Info						
	Board ID:	TriWave					
Device Info	Build Timestamp:	140903_1200					
Advanced Setup	Software Version: 4.14L.04_TLNT_1.4.1						
Wireless	Bootloader (CFE) Version: 1.0.38-117.113						
Diagnostics	Wireless Driver Version: 6.37.14.4803.cpe4.14L04.0-kdb						
Management	Voice Service Version:	Voice					
	Uptime: 0D 0H 11M 445						
	This information reflects the	current status of your WAN connection.					
	LAN IPv4 Address:	192.168.1.1					
	Default Gateway:						
	Primary DNS Server:	0.0.0.0					
	Secondary DNS Server:	0.0.0.0					
	LAN IPv6 ULA Address:						
	Default IPv6 Gateway:						
	Date/Time:	Thu Jan 1 00:11:44 1970					

Información de dispositivo

El interfaz de usuario Web está dividido en dos paneles, el menú principal (a la izquierda) y ventana de contenidos (a la derecha). El menú principal tiene varias opciones y seleccionando cada una de ellas se abrirá un submenú con más opciones a seleccionar.

"Device Info" es la primera selección del menú principal y la primera en mostrarse. Posteriormente se mostrará una introducción.

Device Info



El primer submenú "Device Info Summary" muestra la información relativa al hardware, software, configuración IP,...

WAN

Se muestran los circuitos virtuales permanentes (PVCs) configurados.



Título	Descripción
Interface	Nombre del interfaz WAN
Description	Nombre de la conexión WAN
Туре	Muestra los tipos de conexión
VlanMuxId	Muestra el ID 802.1q de la VLAN
IPv6	Direccionamiento IPv6 habilitado/ deshabilitado
IGMP Proxy	Muestra el estado de Internet Group Management Protocol (IGMP)
IGMP Source Enabled	
MLD Proxy	
MLD Source Enabled	
NAT	Muestra el estado de Network Address Translation (NAT)
Firewall	Muestra el estado del Firewall
Status	Muestra el estado de conexión PON
IPv4 Address	Muestra la dirección IPv4 para el interfaz WAN
IPv6 Address	Muestra la dirección IPv6 para el interfaz WAN

Statistics

Estadísticas. En esta sección se muestran las estadísticas facilitadas por los diferentes interfaces LAN, WAN e interfaz óptico (GPON). En cada uno de los interfaces se mostrarán los siguientes campos:

	Título	Descripción
Interfaz		Nombre del interfaz
		Recibidos
Total		
	- Bytes	Nº Bytes recibidos
	- Pkts	Nº de paquetes recibidos
	- Errs	Nº de paquetes recibidos con errores
	- Drops	Nº de paquetes recibidos descartados
Multicast		
	- Bytes	Nº Bytes multicast recibidos
	- Pkts	№ de paquetes multicast recibidos
Unicast		
	- Pkts	Nº de paquetes unicast recibidos
Broadcast		
	- Pkts	№ de paquetes broadcast recibidos
		Transmitidos
Total		
	- Bytes	Nº Bytes transmitidos
	- Pkts	Nº de paquetes transmitidos
	- Errs	Nº de paquetes transmitidos con errores
	- Drops	Nº de paquetes transmitidos descartados
Multicast		
	- Bytes	Nº Bytes multicast transmitidos
	- Pkts	Nº de paquetes multicast transmitidos
Unicast		
	- Pkts	Nº de paquetes unicast transmitidos
Broadcast		
	- Pkts	Nº de paquetes broadcast transmitidos

LAN

Estadísticas interfaces LAN.



WAN

Estadísticas interfaces WAN.



Route

Tabla de enrutamiento. Rutas dadas de alta en la generación de los diferentes servicios (datos, IPTV, voz,...).



Título	Descripción
Destination	Red/Host de destino
Gateway	Puerta de enlace
Subnet Mask	Máscara de subred de destino
Flag	U: ruta está activa
	!: ruta rechazada
	G: Gateway en uso
	H: el objetivo es un host
	R: restablecer la ruta para enrutamiento dinámico
	D: redirección o subred para configuración dinámica.
	M: Modificado desde la subred enrutada o redirigida
Metric	Muestra el estado de Internet Group Management Protocol
	(IGMP)
Service	Muestra el estado de Network Address Translation (NAT)
Interface	Muestra el interfaz de salida hacia la red

ARP



Campo	Descripción
IP Address	Dirección IP del host
Flags	Complete, Incomplete, Permanent o Publish
HW Address	Dirección MAC del host
Device	Interfaz de conexión

DHCP

Seleccione DHCP para mostrar todos los "DHCP Leases".



Сатро	Descripción
Hostname	Nombre del dispositivo/host en la red
MAC Address	Dirección MAC del dispositivo/host
IP Address	Dirección IP del dispositivo/host
Expires in	Tiempo que queda para la reasignación de la dirección IP del dispositivo/host a través de DHCP

Configuración Avanzada

En este capítulo detallaremos las opciones avanzadas configurables a través de la web.

Layer2 Interface

En esta pantalla podremos modificar la configuración de capa 2 de los interfaces WAN del equipo, tanto GPON como Ethernet:

Campo	Descripción
Interface	ETH WAN Ó GPON WAN
Connection Mode	Default Mode – Único servicio para una conexión Vlan Mux Mode – Múltiples servicios de VLAN para una conexión MSC Mode – Múltiples servicios para una conexión
Remove	Seleccionar la casilla de verificación y haga clic para eliminar la conexión.

GPON interface



WAN Service

🕒 Fiber Home Gateway 🛛 🗙	-		5	-	and the second second	1000	-	-							
← → C ń 🕼 😹 🕹 🕹 🕹 🕹 🕹 🕹 🕹 🕹 🕹 🕹 🕹 🕹															
M movistar												111	111	///	111
					Choose A	Wia ód, Remove	de Area Netwo or Edit to conlig	rk (WAN) Serv	ce Setup ce over a l	elected into	erface.				
Device Info	Interface	Description	Type	Vlan8021p	VlanHuxId	VlanTpid	Igmp Proxy	Igmp Source	NAT	Firewall	IPv6	Hid Proxy	Hid Source	Remove	Edit
dvanced Setup Laver2 Interface	veip0.3	3	1PuE	4	3	0+9100	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	Disabled		Edit
GPON Interface WAN Service	ppp0.1	6	PPP _O E	1	6	0x8100	Disabled	Disabled	Enabled	Enabled	Brabled	Disabled	Disabled	8	Edt
LAN Security Security Control Quality of Service Konting OHS OHS Paray IP Tomet Philocast Infendes Gapredics Sampedics							Add	Remove							

Título	Descripción
Interface	Nombre del interfaz WAN
Description	Nombre de la conexión WAN
Туре	Muestra los tipos de conexión
Vlan8021p	Muestra la prioridad 802.1p
VlanMuxId	Muestra el ID 802.1q de la VLAN
IGMP Proxy	Muestra el estado de Internet Group Management Protocol Proxy (IGMP Proxy)
IGMP Source	Muestra el estado de Internet Group Management Protocol Source (IGMP Source)
NAT	Muestra el estado de Network Address Translation (NAT)
Firewall	Muestra el estado del Firewall
IPv6	Muestra si tiene habilitada la funcionalidad IPv6
MLD Proxy	Muestra si tiene habilitada la funcionalidad de IPv6 <i>Multicast Listener</i> <i>Discovery Proxy</i> (MLD Proxy)
MLD Source	Muestra si tiene habilitada la funcionalidad de IPv6 <i>Multicast Listener</i> <i>Discovery Source</i> (MLD Source)
Remove	Seleccionar la casilla de verificación y haga clic para eliminar la conexión.
Edit	Hacer clic sobre el botón para modificar los valores de los campos

LAN

Local Area Network (LAN) Setup. Esta sección permite la visualización y modificación de valores del interfaz LAN. A continuación se muestra la pantalla que aparece, así como una pequeña descripción de los parámetros.



Título	Descripción
IP Address	Introduzca la dirección IP para el interfaz LAN
Subnet Mask	Introduzca la máscara de subred del interfaz LAN
Enable IGMP Snooping	Si el check está activado, habilita la funcionalidad IGMP Snooping

Standard Mode	El tráfico multicast inundará todos los puertos cuando no haya ningún
	cliente suscrito a un grupo multicast, incluso si IGMP snooping está
	activado.
BIOCKING WIODE	El trafico de datos multicast sera bioqueado y no inundara todos los
	puertos
Enable IGMP LAN to	Si está chequeado se habilita esta opción.
LAN Multicast	
Enable LAN side firewall	Marcar esta casilla para activarlo.
Disable/Enable DHCP	Para activar el DHCP, seleccione Enable DHCP server e introduzca la
Server	dirección IP de inicio y de final del rango y el tiempo de préstamo de
	dirección IP (Leased Time). Estos parámetros configuran el router para
	asignar automáticamente dirección IP, puerta de enlace por defecto y
	servidores DNS a cada PC de la LAN
Static IP Lease List:	Pueden ser configuradas un máximo de 32 entradas. Haciendo clic sobre el
	botón "Add Entries". En la siguiente pantalla se deberá asignar a la
	dirección MAC correspondiente la dirección IP deseada. Con el Botón
	"Remove Entries" se eliminarán las entradas con el check Remove
	habilitado.
Configure the second IP	Si se desea una segunda dirección IP en el interfaz WAN se debe habilitar
Address	esta opción
IP Address	Introduzca la dirección IP secundaria de la LAN.
Subnet Mask	Introduzca la máscara de red para la IP secundaria de la LAN.

IPv6 AutoConfig

DHCPv6 está soportado bajo la premisa de un longitud del prefijo menor que 64. Interface ID no soporta comprensión de ceros "::". Introduce la información completo. Ejemplo: "0:0:0:2" en lugar de "::2"



Título	Descripción
Interface Address	Dirección IPv6 del interfaz. Es necesario indicar la longitud del prefijo
	IPv6 LAN Applications
Enable DHCPv6 Server	.Seleccionar está opcion habilita la funcionalidad de servidor DHCPv6, permitiendo seleccionar el modo stateless o stateful.
Stateless	En esta configuración, el host utiliza el prefijo (la dirección de red y la máscara de subred), el cual es "publicado" por los dispositivos de red como parte de la creación de la dirección. Posteriormente los clientes pueden utilizar su dirección física (<i>MAC address</i>) para completar la identificación del dispositivo y así asignar la dirección IPv6.

Stateful	Es un metodo similar al DHCP en IPv4, en este modo se deben definir los							
	IDs de inicio y fin así como el tiempo en horas que se mantendrá la							
	dirección IPv6 generada hasta una nueva actualización de la dirección							
	(leased time)							
Enable RADVD	Habilita el Router Adversitement Daemon							
Enable ULA Prefix	Habilita/deshabilita el anuncio de prefijos ULA. Pueden ser generado							
Advertisement	aleatoria o estáticamente.							
Randomly Generate	El anuncio de prefijos será aleatorio							
Statically Configure	Los prefijos serán configurados estáticamente. Habrá que configurar los							
	siguientes parámetros: "Prefix", "Preferred Life Time" y "Valid Life Time".							
Prefix	Valor del prefijo							
Preferred Life Time	Tiempo de vida favorito en horas							
(hour)								
Valid Life Time (hour)	Tiempo de vida valido en horas							
Enable MLD Snooping	Si está chequeado, habilita el protocolo MLD							
Standard Mode	El tráfico multicast inundará todos los puertos cuando no haya ningún							
	cliente suscrito a un grupo multicast, incluso si IGMP snooping está							
	activado.							
Blocking Mode	El tráfico de datos multicast será bloqueado y no inundará todos los							
	puertos							

NAT

Virtual Servers

Virtual Servers o servidores virtuales permiten redirigir el tráfico entrante desde la WAN (identificando Protocolo y Puerto externo) a un servidor interno con dirección privada en el lado de la LAN. Los puertos internos son requeridos solo si el Puerto externo necesita ser convertido a un Puerto interno diferente para ser usado por el servidor interno del lado de la LAN.

Pueden ser configuradas un máximo de 32 entradas.

Fiber Home Gateway	
← → C fi Beben	۶/192168.11:8080/main.html
Person and Person and Anomed Setup Advanced Setup Advanced Setup Advanced Setup Advanced Setup Advanced Setup Advanced Setup Advanced Ad	AIT - Vortaal Serveral Seland I data was allow anyo to direct tooming halfs from 1988 the lot bestow and to be total and a server of the LMI seles. A maximum I data is a lot and a lot of select and point Select and Destinal and units to the lot and a lot of select and point Select and a server of the LMI select. A maximum I data is a lot and a lot of select and point Select
Particle Control Quality of Service Routing DMS UPuP DMS Proxy IP Tunnel Multicat. Workers Voice Diagnowtics Management	

Para añadir un "Virtual Server", haga clic en el botón "Add". Se mostrará la siguiente pantalla:

Fiber Home Gateway ×		-	-	- Married	to star	
+ -> C fi (s beros)	/192.168.1.1:808	0/main.html				t i i i i i i i i i i i i i i i i i i i
M movistar			0.000			
	NAT Virtual Server	-				
Device Info Advanced Setup	Select the service name Start", then "Interna Remaining number of	e, and enter the serv al Port End" will be of entries that can	er IP address and e set to the same be configured:3	dick "Apply/Seve" to value as "Internal 2	forward IP packats fo Port Start",	c bis service to the specified server. NOTE: The "Internal Port End" cannot be modified directly, Normally, it is set to the same value as "External Port End". However, if you modify "Internal Port
Layer2 Interface	Use Interface	3/velp0.3 •				
LAN	Select a Service	Select One				
NAT	Custom Service:	. See a second s				
Virtual Servers Port Triggering DHZ Host	Server IP Address:	192.160.1.				
Security Parental Control						/Apply/Save
Quality of Service	Fature 1 Read Fit and	Colored Real Field	Basharal	Tota and Bash Stre	differenced Read Free	
Routing	Extensi Port Starts	External Port End	TCP .	Anternal Port Stat	NUMBER AND POPLEM	
UPnP			TCP T			
DNS Proxy			TOD -			4
IP Tunnel Multicast			TUP ·		-	
Wireless			TCP •			
Voice			TCP •			
Diagnostics			TCP .			
			TCP .			
			TCP *			
			TCP .			
			TOP .			
			TOP T			4
			TCP V			4
			TCP •]
						Apple/Serve

Título	Descripción
Use Interface	Seleccione el interfaz WAN de la lista desplegable
Select a service/	Seleccione un servicio de la lista desplegable o cree un servicio personalizado
Custom Server	introduciendo un nombre
Server IP Address	Introduzca la dirección IP del servidor interno
External Port Start	Introduzca el puerto externo de inicio de rango (cuando seleccione un servicio
	personalizado o "Custom Server"). Cuando un servicio es seleccionado, el
	rango de puertos se configura automáticamente.
External Port End	Introduzca el puerto externo de fin de rango (cuando seleccione un servicio
	personalizado o "Custom Server"). Cuando un servicio es seleccionado, el
	rango de puertos se configura automáticamente.
Protocol	TCP, UDP, TCP/UDP
Internal Port Start	Introduzca el puerto interno de inicio de rango (cuando seleccione un servicio
	personalizado o "Custom Server"). Cuando un servicio es seleccionado, el
	rango de puertos se configura automáticamente.
Internal Port End	Introduzca el puerto interno de fin de rango (cuando seleccione un servicio
	personalizado o "Custom Server"). Cuando un servicio es seleccionado, el
	rango de puertos se configura automáticamente.

Port Triggering

Algunas aplicaciones requieren que los puertos cuenten con acceso permitido en el firewall. *Port Triggers* dinámicamente "abre los puertos" en el firewall sólo cuando la aplicación del lado de la LAN inicia la conexión TCP/UDP a un sitio remoto usando "*triggering Ports*". El router permite al sitio remoto desde el lado de la WAN establecer nuevas conexiones a la aplicación del lado de la LAN usando los "puertos abiertos".

Pueden ser configuradas un máximo de 32 entradas.



Para añadir un "Trigger Port", haga clic en el botón "Add". Se mostrará la siguiente pantalla:

Fiber Home Gateway		-		-		1	
← → C fi & beeps	//192.168.1.1:8080/mi	ain.html					
M movistar							
Device Info Advanced Setup Layer2 Interface WAN Service LAN	NAT → Port Triggering Some applications such as gar dick. Save/Apply to add R. Remaining number of entr Use Interface Application Hames	nes, video conference tes that can be co 3/veip0.3 ¥ Select One	ing, remote ofigured: 3	access application	ons and others r	eoure that sp	specific ports in the Router's frewall be spaned for access by the applications. You can configure the port settings from this access by selecting an existing application or overing your own (Custom application)
NAT Virtual Servers Port Triggering DMZ Host	Custom application						[Second Apply]
Security Reported Control	Tripper Part Start Tripper	Port End Trigger	Protocol 0	Open Port Start	Open Port En	d Open Pro	relaced
Quality of Service		TCP	-		-	TCP	
Routing		TCP	•		-	TCP	•
UPnP		TCP	•			TCP	•
DNS Proxy		TCP	•	- S		TCP	•
IP Tunnel Multicast		TCP				TCP	•
Wireless		TCP	•			TCP	•
Voice		TCP	•		1	TCP	
Diagnostics Management		TCP				TCP	
							Secularly.
Título	Descripción						
------------------------	---						
Use Interface	Seleccione el interfaz WAN de la lista desplegable						
Select an Application/	Seleccione una aplicación de la lista desplegable o cree una aplicación						
Custom Application	personalizada introduciendo un nombre						
Trigger Port Start	Introduzca el puerto Trigger de inicio de rango (cuando seleccione una						
	aplicación personalizada o "Custom Server"). Cuando una aplicación es						
	seleccionada, el rango de puertos se configura automáticamente.						
Trigger Port End	Introduzca el puerto Trigger de fin de rango (cuando seleccione una						
	aplicación personalizada o "Custom Server"). Cuando una aplicación es						
	seleccionada, el rango de puertos se configura automáticamente.						
Trigger Protocol	TCP, UDP, TCP/UDP						
Open Port Start	Introduzca el puerto abierto de inicio de rango (cuando seleccione una						
	aplicación personalizada o "Custom Server"). Cuando una aplicación es						
	seleccionada, el rango de puertos se configura automáticamente.						
Open Port End	Introduzca el puerto abierto de fin de rango (cuando seleccione una						
	aplicación personalizada o "Custom Server"). Cuando una aplicación es						
	seleccionada, el rango de puertos se configura automáticamente.						
Open Protocol	TCP, UDP, TCP/UDP						

DMZ Host

TriWave permite el paso del lado WAN hacia el Host DMZ, a aquellos paquetes que no pertenezcan a aplicaciones configuradas en la tabla de "Virtual Server".

1 :8080/r	'mai	ain	ain	in																		_																		
						Ir	In	n.	h.ht	ntn	ml	1																												
Hart																																								
me Gateway v	will for	forv	forw	orv	or	or	orv	rwa	varo	rd II	IP p	pac	ckets	ts fro	om t	the W	WAN	l tha	t do	o no	ot be	lon	g to	any	oft	he a	pplic	atior	s con	figure	d in t	he Vi	rtual !	Server	s tabl	e to ti	ne DM2	? host	comp	outer.
mputer's IP ad address field a Address:	ddress and cli	ess a clid	ss a click	as a clic			s a flich	i an	and k 'A	d cli	lick ply	c 'Ap	pply dea	y' to	> acti	the I	the DM2	EDM.	IZ hi	ost.																	Sa	ve/Ap	ply	
HI2 Ho	42 Host Home Gateway computer's IP a P address field IP Address:	4Z Host Home Gateway will computer's IP addre P address field and IP Address:	4Z Host Home Gataway will I computer's IP addres P address field and IP Address:	4Z Host Home Gateway will f computer's IP address P address field and d IP Address:	4Z Host Home Gateway will f computer's IP address P address field and d IP Address:	4Z Host Home Gateway will f computer's IP address P address field and d IP Address:	4Z Host Home Gateway will fi computer's IP address P address field and o IP Address:	4Z Host Home Gateway will fo computer's IP address P address field and cl IP Address:	4Z Host Home Gateway will fon computer's IP address i P address field and clic IP Address:	12 Host Home Gateway will forwa computer's IP address an P address field and click IP Address:	4Z Host Home Gateway will forward computer's IP address and ci P address field and click 'Ap IP Address:	4Z Host Home Gateway will forward IP computer's IP address and click P address field and click 'Apply IP Address:	4Z Host Home Gateway will forward IP pa computer's IP address and click 'A P address field and click 'Apply' tr IP Address:	42 Host Home Gateway will forward IP packet computer's IP address and click 'Apply' to de IP Address:	4Z Host Home Gateway will forward IP packets fr computer's IP address and click 'Apply' to P address field and click 'Apply' to deact IP Address:	4Z Host Home Gateway will forward IP packets from I computer's IP address and click 'Apply' to act P address field and click 'Apply' to deactivate IP Address:	4Z Host Home Gateway will forward IP packets from the h computer's IP address and click 'Apply' to activate P address field and click 'Apply' to deactivate the IP Address:	AZ Host Home Gateway will forward IP packets from the WAA computer's IP address and click 'Apply' to deactivate the P address field and click 'Apply' to deactivate the DM IP Address:	4Z Host Home Gateway will forward IP packets from the WAN that computer's IP address and click 'Apply' to activate the DMZ ho P address field and click 'Apply' to deactivate the DMZ ho IP Address:	4Z Host Home Gateway will forward IP packets from the WAN that do computer's IP address and click 'Apply' to activate the DMZ h P address field and click 'Apply' to deactivate the DMZ host. IP Address:	4Z Host Home Gateway will forward IP packets from the WAN that do no computer's IP address and click 'Apply' to activate the DM2 host. P address field and click 'Apply' to deactivate the DM2 host. IP Address:	4Z Host Home Gateway will forward IP packets from the WAN that do not be computer's IP address and click 'Apply' to activate the DMZ host. P address field and click 'Apply' to deactivate the DMZ host. IP Address:	AZ Host Home Gateway will forward IP packets from the WAN that do not belon computer's IP address and click 'Apply' to activate the DMZ host. P address field and click 'Apply' to deactivate the DMZ host. IP Address:	AZ Host Home Gateway will forward IP packets from the WAN that do not belong to computer's IP address and click 'Apply' to activate the DM2 host. P address field and click 'Apply' to deactivate the DM2 host. IP Address:	4Z Host Home Gateway will forward IP packets from the WAN that do not belong to any computer's IP address and click 'Apply' to activate the DMZ host. P address field and click 'Apply' to deactivate the DMZ host. IP Address:	AZ Host Home Gateway will forward IP packets from the WAN that do not belong to any of the computer's IP address and click 'Apply' to activate the DMZ host. P address field and click 'Apply' to deactivate the DMZ host. IP Address:	AZ Host Home Gateway will forward IP packets from the WAN that do not belong to any of the a computer's IP address and click 'Apply' to activate the DMZ host. P address field and click 'Apply' to deactivate the DMZ host. IP Address:	AZ Host Home Gateway will forward IP packets from the WAN that do not belong to any of the applic computer's IP address and click 'Apply' to activate the DMZ host. P address field and click 'Apply' to deactivate the DMZ host. IP Address:	AZ Host Home Gateway will forward IP packets from the WAN that do not belong to any of the application computer's IP address and click 'Apply' to activate the DMZ host. P address field and click 'Apply' to deactivate the DMZ host. IP Address:	AZ Host Home Gateway will forward IP packets from the WAN that do not belong to any of the applications concomputer's IP address and click 'Apply' to activate the DMZ host. P address field and click 'Apply' to deactivate the DMZ host. IP Address:	AZ Host Home Gateway will forward IP packets from the WAN that do not belong to any of the applications configure computer's IP address and click 'Apply' to activate the DMZ host. P address field and click 'Apply' to deactivate the DMZ host. IP Address:	AZ Host Home Gateway will forward IP packets from the WAN that do not belong to any of the applications configured in toopputer's IP address and click 'Apply' to activate the DMZ host. P address field and click 'Apply' to deactivate the DMZ host. IP Address:	AZ Host Home Gateway will forward IP packets from the WAN that do not belong to any of the applications configured in the Viccomputer's IP address and click 'Apply' to activate the DMZ host. P address field and click 'Apply' to deactivate the DMZ host. IP Address:	AZ Host Home Gateway will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual ! computer's IP address and click 'Apply' to activate the DMZ host. P address field and click 'Apply' to deactivate the DMZ host. IP Address:	AZ Host Home Gateway will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Server computer's IP address field and click 'Apply' to activate the DMZ host. P address field and click 'Apply' to deactivate the DMZ host. IP Address:	AZ Host Home Gateway will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table computer's IP address field and click 'Apply' to activate the DMZ host. P address field and click 'Apply' to deactivate the DMZ host. IP Address:	AZ Host Home Gateway will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the computer's IP address field and click 'Apply' to activate the DMZ host. P address field and click 'Apply' to deactivate the DMZ host. IP Address:	AZ Host Home Gateway will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DM2 computer's IP address and click 'Apply' to activate the DM2 host. P address: D Address: Sa	AZ Host Home Gateway will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer's IP address and click 'Apply' to activate the DMZ host. IP Address: Save/Ap	AZ Host Home Gateway will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host comp computer's IP address and click 'Apply' to activate the DMZ host. IP address: Save/Apply

Para activar el Host DMZ, introduzca la dirección IP y haga clic en el botón "Save/Apply".

Para desactivar el host DMZ, borre la dirección IP y haga clic en el botón "Save/Apply".

Security

Para que esta opción esté disponible, debe estar habilitado el firewall en la configuración WAN.

IP Filtering Outgoing

Esta opción permite configurar filtros o reglas que limitan el tráfico IP de salida. Múltiples reglas de filtrado pueden ser configuradas y aplicadas en cada una al menos con una condición de limitación. Para paquetes IP individuales para pasar el filtro debe cumplir cada una de las condiciones.

Por defecto, todo el tráfico IP saliente está permitido, pero este tráfico IP puede ser bloqueado con filtros.



Para añadir un filtro (para bloquear tráfico IP saliente), haga clic en el botón "Add". En la siguiente pantalla, introduzca los criterios de filtrado y haga clic en el botón "Apply/Save".

🖉 🖹 Fiber Home Gateway	×	Statements of the local division in the loca	The diversity of the section	sufficient State State	- In Street & Support to the	Concession in which the real Property lies in which the real property lies in the real property	
← → C fi @sbatt	5://192.168.1.1:8080/main.ht	tml					
	Add IP Filter Outgoing The screen allows you to create a filt	ar rule to identify outgoing 17	P traffic by specifying a new filter name and	I at least one condition below. All of the	specified conditions in this filter rule n	ut be satafied for the rule to take effect	. click /qppl/Save' to save and activate the filter.
Device Info Advanced Setup Layer2 Interface WAM Service LAN NAT Security IIF Filtering Outgoing Incoming Parental Central Quality of Service Routing DMS DMS DMS DMS Proxy IIF Tumonit Multicast Workes Voice Diagonastics Hanagement	Filter Name: 19 Version Protocil: Servar D address(jarefis length); Soraro Rot (joot ar potopot); Destinuation State(jarefis length); Destinuation Rot (joot ar potopot);		•		AppleSam		

Campo	Descripción
Filter Name	Introduzca el nombre del filtro
IP Version	IPv4, IPv6
Protocol	TCP, UDP, TCP/UDP, ICMP
Source IP Address[/prefix length]	Introduzca la dirección IP origen. Si se trata de una red se puede añadir la máscara.
Source Port (port or port:port)	Introduzca el número de puerto origen o el rango de puertos origen.
Destination IP Address[/prefix length]	Introduzca la dirección IP destino. Si se trata de una red se puede añadir la máscara.
Destination Port (port or port:port)	Introduzca el número de puerto destino o el rango de puertos destino.

IP Filtering Incoming

Por defecto, todo el tráfico entrante está bloqueado, pero puede ser permitido creando filtros.

	://192.168.1.1:8080/main.html									
	Incoming IP Filtering Setup								////	
	When the firewall is enabled on a WAN or LAN interface, all incomi	ng IP traffic is BLOCKED. However, some IP	traffic can be	ACCEPTED	y setting up	o filters.				
Device Info	Choose Add or Remove to configure incoming IP filters.									
Advanced Setup Layer2 Interface		Filter Name	Interfaces	IP Version	Protocol	SrcIP/ PrefixLength	SrcPort	DstIP/ PrefixLength	DstPort	Remov
WAN Service		PPP_INPUT.1	ppp0.1	4	ICMP					
LAN		DOD THOUT 3			700	102 152 27 102/20			445	
Security		PPP_INPUT.2	ppp0,1		TOP	193,152,37,192/28			443	
IP Filtering		PPP_INPUT.3	ppp0.1	4	TCP	193.152,37.192/28			22	
Outgoing		PPP_INPUT.4	ppp0.1	4	TCP	172.20.25.0/24			22	
Parental Control								-		-
Quality of Service		PPP_INPUT.5	ppp0.1	4	TCP	172.20.25.0/24			443	
DNS		PPP_INPUT.6	ppp0.1	4	TCP	172.20.45.0/24			22	
UPnP		PPP INPUT.7	ppp0.1	4	тср	172.20.45.0/24			443	
DNS Proxy				12.0					1.10	-
IP Tunnel Multicast		PPP_INPUT.8	ppp0.1	4	TCP	80.58.63.128/25			22	
Wireless		PPP_INPUT.9	ppp0.1	4	TCP	80.58.63.128/25			443	
		PPD TNDUT 10	npn0.1	4	TCP	80.58.63.128/25			7547	
Voice		PPP_INPOTIZO	PPP-14	8	1979 A	000000000000000				
Voice Diagnostics Management		TO ME SHOW TO A MARK THE SHOW	1.1.1.1							

Para añadir un filtro (para permitir tráfico entrante), haga clic en el botón "Add". En la siguiente pantalla, introduzca los criterios de filtrado y haga clic en el botón "Apply/Save".

📕 📄 Fiber Home Gateway	
← → C fi as bat	p\$//192.168.1.1:8080/main.html
	Add IP Filter Incoming
Device Info Advanced Setup Layez Interface WAN Service LAN NAT Security IP Filtering Outgoing Incoming Parental Control Quality of Service Routing DNS UPAP DNS Proxy ID Tunnel Multicast Wireless Voice Diagnostics Management	The screen allow you to create a filter rule to skettly incorting IP tattic by spectrying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter. Filter Name: IP Version: IP Versio

Сатро	Descripción
Filter Name	Introduzca el nombre del filtro
IP Version	ΙΡν4, ΙΡν6
Protocol	TCP, UDP, TCP/UDP, ICMP
Source IP Address[/prefix length]	Introduzca la dirección IP origen. Si se trata de una red se puede añadir la máscara.
Source Port (port or port:port)	Introduzca el número de puerto origen o el rango de puertos origen.
Destination IP Address[/prefix length]	Introduzca la dirección IP destino. Si se trata de una red se puede añadir la máscara.
Destination Port (port or port:port)	Introduzca el número de puerto destino o el rango de puertos destino.

En la imagen superior, seleccione el interfaz WAN y LAN en los que serán aplicados las reglas de filtrado. Debe seleccionar todos o solo un subconjunto. Con interfaces WAN en modo bridge o sin firewall activado no estará disponible.

Parental Control

Esta sección permite establecer determinadas restricciones a determinados horarios y determinadas webs. A continuación detallamos estas funcionalidades.

Time Restriction

Esta característica restringe el acceso desde un dispositivo LAN a un lugar en el exterior de la red a determinadas horas en los días seleccionados. Para asegurar que esta funcionalidad está activa, la sincronización "Internet Time server" o NTP debe estar activado como se indica en el apartado correspondiente, de modo que los periodos de tiempo seleccionados coincida con su hora local.



Haga clic en el botón "Add" para mostrar la siguiente pantalla.



Haga clic en el botón "Save/Apply" para añadir un periodo de restricción.

Ver la descripción de campos a continuación.

Campo	Descripción
User Name	Nombre definido por el usuario para la restricción
Browser's MAC Address	Dirección MAC del PC que inicia su navegador
Other MAC Address	Dirección MAC de otro dispositivo LAN
Days of the Week	Los días en que la restricción será aplicada
Start Blocking Time	El tiempo de inicio la restricción
End Blocking Time	El tiempo de finalización de la restricción

URL Filter

Este menú permite la creación de reglas de filtrado basado en direcciones web o URL y el número de puerto para tener derechos de acceso.



Haga clic en el botón "Add" para mostrar la siguiente pantalla.



Para la creación de un filtro a una URL, seguir los siguientes pasos:

Paso 1: Introduzca la dirección URL y número de puerto y posteriormente haga clic en el botón "*Save/Apply*" para añadir la entrada al filtro URL. La dirección URL comienza por "www", como se muestra en este ejemplo:

/ 🕒 Fiber Home Gateway 🛛 ×	sales in the R officers
← → C f (k) (192.168.1.1:8080/main.html	
C n RAMES://192.168.1.1:8080/main.ntml Mile and a second	Address Port Remove www.teinet-ri.es 80

Se pueden añadir un máximo de 100 entradas a la lista de filtrado URL.

Paso 2: Especificar tipo de filtro. Marque "*Exclude*" para sólo permitir el acceso a los sitios de internet enumerados. Marque "*Include*" para restringir el acceso únicamente a los sitios de internet enumerados.

Quality of Service

Si el check "Enable QoS" está seleccionado, elige una etiqueta DSCP por defecto para marcar el tráfico entrante sin referencia a una clasificación particular. Haz clic sobre el botón "Apply/Save" para guardar los cambios.

Nota: Si el *check* "Enable QoS" no está seleccionado, QoS será deshabilitado en todos los interfaces.

Nota: La etiqueta DSCP por defecto se utiliza para marcar todo el tráfico saliente que no ha pasado por ninguna regla de clasificación.



QoS Queue

En modo ATM, un máximo de 16 colas de prioridad se pueden configurar.

En cada interfaz Ethernet, hasta un máximo de 8 colas pueden configurarse, igual que en los interfaces WAN Ethernet.

En la imagen mostrada a continuación están las colas de prioridad que están generadas en el equipo por defecto. Estas colas no pueden ser eliminadas (no tiene habilitada la opción *"Remove"*) y siempre están habilitadas, salvo que la función WMM está deshabilitada en la página *"Wireless"*, entonces las colas relativas al interfaz *wireless* no tomarán efecto.

		5/1110	manaru				_					
M movistar												
Q	oS Queue Setup											
In	ATM mode, maximu	m 16 qu	eues can be	configu	red.							
evice Info	or each Ethernet inter	interfa	aximum 8 que	eues ca	n be configured.	4						
dvanced Setun	add a queue, click ti	ne Add	button.	~ queu	na can be connighted							
Laver2 Interface	remove queues, che	ck thei	r remove-chec	kboxes	, then click the Rem	ove button.						
Layer & Anternace	to remove queues, cneck mer remove-cneckboxes, men click me kemove outcon. The Enable button will scan through every queues in the table. Queues with enable-checkbox checked will be enabled. Queues with enable-checkbox un-checked will be disabler											
WAN Service	ne enable-checkbox a	en cho	we statue of th	10 (110)	in after page reload							
WAN Service Th	ne enable-checkbox a ote that if WMM funct	ion is d	ws status of th isabled in Win	ne queu eless Pa	ie after page reload. age, queues related I	to wireless will not take	effects.					
WAN Service Ti LAN No NAT F	ne enable-checkbox a ote that if WMM funct	so sho ion is d	ws status of th isabled in Wir	ne queu eless P	ie after page reload. age, queues related I	to wireless will not take	effects.		•			
WAN Service The North Service The North Security	ne enable-checkbox a ote that if WMM funct Name	ion is d Key	ws status of th isabled in Win Interface	ne queu eless Pi Qid	e after page reload. age, queues related i Prec/Alg/Wght	to wireless will not take Min Bit Rate(bps)	effects. Enable	Remove				
VAN Service Tr AN No VAT Security Parental Control	ne enable-checkbox a ote that if WMM funct Name	ion is d	ws status of th isabled in Win Interface	eless P Qid	e after page reload. age, queues related i Prec/Alg/Wght	to wireless will not take Min Bit Rate(bps)	effects. Enable	Remove				
VAN Service Tr AN No VAT Security Parental Control Quality of Service	ne enable-checkbox a ote that if WMM funct Name WMM Voice Priority	ion is d Key	ws status of th isabled in Wir Interface wl0	eless P Qid 8	e after page reload. age, queues related f Prec/Alg/Wght 1/SP	to wireless will not take Min Bit Rate(bps)	effects. Enable Enabled	Remove				
WAN Service TT LAN N NAT Security Parental Control Quality of Service CoS Queue	ne enable-checkbox a ote that if WMM funct Name WMM Voice Priority WMM Voice Priority	Key 1	ws status of th isabled in Win Interface wl0 wl0	Qid 8	Prec/Alg/Wght 1/SP 2/SP	to wireless will not take Min Bit Rate(bps)	effects. Enable Enabled Enabled	Remove				
WAN Service Tr LAN No. NAT Security Parental Control Quality of Service QOS Queue QOS Classification	ne enable-checkbox a ote that if WMM funct Name WMM Voice Priority WMM Voice Priority	Key	ws status of the sabled in Wine Interface wild wild wild wild wild wild wild wild	Qid 8 7	Prec/Alg/Wght 1/SP 2/SP 2/CD	to wireless will not take	effects. Enable Enabled Enabled	Remove				
WAN Service Tr LAN No NAT Security Parental Control Quality of Service Quality of Service QoS Classification Routing Cos Classification Cos Classi	ne enable-checkbox a tote that if WMM funct Name WMM Voice Priority WMM Voice Priority WMM Video Priority	Key 1 2 3	ws status of the status of the status of the state of the	Qid 8 7 6	e after page reload. age, queues related I Prec/Alg/Wght 1/SP 2/SP 3/SP	to wireless will not take	effects. Enable Enabled Enabled Enabled	Remove				
WAN Service TT LAN NAT Security Quality of Service QoS Queue QoS Classification Routing DNS	ne enable-checkbox a obe that if WMM funct Name WMM Voice Priority WMM Voice Priority WMM Video Priority WMM Video Priority	Key 1 2 3 4	ws status of the	Qid 8 7 6 5	e after page reload, age, queues related I Prec/Alg/Wght 1/SP 2/SP 3/SP 4/SP	to wireless will not take Min Bit Rate(bps)	effects. Enabled Enabled Enabled Enabled	Remove				
WAN Service TT LAN NAT Security Quality of Service Quality of Service QoS Classification Routing DNS DNS UPnP	Name WMM Voice Priority WMM Voice Priority WMM Voice Priority WMM Video Priority	Key 1 2 3 4	ws status of the	Qid 8 7 6 5	e after page reload, age, queues related I Prec/Alg/Wght 1/SP 2/SP 3/SP 4/SP	to wireless will not take Min Bit Rate(bps)	effects. Enable Enabled Enabled Enabled Enabled	Remove				
WAN Service Tr LAN Not Security Parental Control Quality of Service QoS Classification Routing DNS UPAP UPAP DNS DNS	ne enable-checkbox a ote that if WMM funct Name WMM Voice Priority WMM Video Priority WMM Video Priority WMM Video Priority WMM Best Effort	Key 1 2 3 4 5	ws status of the	Qid 8 7 6 5 4	e after page reload, age, queues related i Prec/Alg/Wght 1/SP 2/SP 3/SP 4/SP 5/SP	to wireless will not take Min Bit Rate(bps)	effects. Enable Enabled Enabled Enabled Enabled Enabled Enabled	Remove				
WAN Service Tr LAN Not NAT Security Parental Control Quality of Service QoS Classification QoS Classification QoS Classification QoS Classification QDNS UPNP DNS Proxy IP Tunnel Multicat	ne enable-checkbox a obe that if WMM funct Name WMM Voice Priority WMM Video Priority WMM Video Priority WMM Video Priority WMM Background	Key 1 2 3 4 5 6	ws status of the	Qid 8 7 6 5 4 3	e after page reload. age, queues related 1 Prec/Alg/Wght 1/SP 2/SP 3/SP 4/SP 5/SP 6/SP	to wireless will not take Min Bit Rate(bps)	effects. Enabled Enabled Enabled Enabled Enabled Enabled Enabled Enabled	Remove				
WAN Service TT LAN NAT Security Quality of Service QoS Queue QoS Classification Routing DNS DNS DNS DNS Poxy IP Tunnel Multicast riceless	ne enable-checkbox a ote that if WMM funct Name WMM Voice Priority WMM Voice Priority WMM Video Priority WMM Video Priority WMM Background WMM Background	Key 1 2 3 4 5 6 7	ws status of the isabled in Win isabled in Win wlo wlo wlo wlo wlo wlo wlo wlo	Qid 8 7 6 5 4 3	re after page reload. age, queues related i 1/SP 2/SP 3/SP 4/SP 5/SP 6/SP 7/S0	to wireless will not take Min Bit Rate(bps)	effects. Enable Enabled Enabled Enabled Enabled Enabled Enabled Enabled Enabled	Remove				
WAN Service TT LAN NAT Security Quality of Service Quality of Service QoS Classification Routing DNS UPnP DNS Proxy IP Tunnel Multicast ireless oice	ne enable-checkbox a tote that if WMM funct Name WMM Voice Priority WMM Voice Priority WMM Video Priority WMM Video Priority WMM Best Effort WMM Background WMM Background	Key 1 2 3 4 5 6 7	vs status of ti vissabled in Winisabled in Winisabled in Winisabled in Winisabled in Winisable with which with which whi	Qid 8 7 6 5 4 3 2	e after page reload. age, queues related i 1/SP 2/SP 3/SP 4/SP 6/SP 7/SP	to wireless will not take Min Bit Rate(bps)	effects. Enable Enabled Enabled Enabled Enabled Enabled Enabled	Remove				
WAN Service TT LAN N NAT Security Parental Control Quality of Service QoS Classification QoS Classification Routing DNS UPnP DNS Proxy IP Tunnel Multicast ireless sice agnostics The Service Control of the S	ne enable-checkbox a obe that if WMM funct Name WMM Voice Priority WMM Video Priority WMM Video Priority WMM Video Priority WMM Background WMM Background WMM Background	Iso sho ion is d 1 2 3 4 5 6 7 8	vs status of tł issabled in Win Interface wło wło wło wło wło wło wło	Qid 8 7 6 5 4 3 2 1	e after page reload. age, queues related i Prec/Alg/Wght 1/SP 2/SP 3/SP 4/SP 5/SP 6/SP 7/SP 8/SP	to wireless will not take Min Bit Rate(bps)	effects. Enabled	Remove				

Para añadir una cola, clic en botón "Add".

Para eliminar colas, selecciona los *checks "Remove"* correspondientes y haz clic sobre el botón *"Remove"* de la parte inferior.

El botón "*Enable*" actualiza las colas. Habilita las colas que tienen el *check* "*Enable*" habilitado y deshabilita las colas con este *check* deshabilitado. Por tanto, para que los cambios en los *checks* "*Enable*" tengan efecto es necesario pulsar el botón "*Enable*" de la parte inferior.

Campo	Descripción
Name	Nombre identificativo de la cola
Кеу	Número identificativo de la cola
Interface	Interfaz de la cola
Qid	Número de cola del interfaz
Prec/Alg/Wght	Valores para la priorización de las colas.
Min Bit Rate (bps)	Bps garantizado en los casos que sea necesario.
Enable	Habilitación/deshabilitación de la cola
Remove	Eliminación de la cola

📔 Fiber Home Gateway	×	Send or otherwise	report for the Lot Sugar in Fight & or
← → C fi 🕑 bttp	s ://192.168.1.1:808	0/main.html	
M movista	r		
	QoS Queue Configu	ation	
	This screen allows you	to configure a QoS queue and add it to a selected layer2 interface.	
Device Info	Name:		
Advanced Setup			
Layer2 Interface	Enable:	Enable *	
WAN Service			
LAN	Interface:	▼	
NAT			
Security			20 million
Parental Control			Apply/Save
Quality of Service			
QoS Queue			
QoS Classification			
Routing			
DNS			
OPhP			
DNS Proxy			
IP Tunnet Multi-set			
Windows			
Voice			
Diagnostics			
Management			

QoS Classification

Para clasificar el tráfico entrante se pueden configurar hasta un total de 32 reglas.

Fiber Home Gateway	· · · · · · · · · · · · · · · · · · ·
← → C A (* beep	≰//192.168.1.1.8080/main.html
M movista	Cycl Classification Serlay
Device Info Advanced Setup Layer2 Interface	The Feedble future off care in triningh every relative - the table. Enders with treatestation of the analysis, Euler with enabled, Euler with enab
WAN Service	CLASSIFICATION CRITERIA CLASSIFICATION RESULTS
LAN	Class Name Order [Class Int] Ether Type SrcMAC/ Mask DotMAC/ Mask SrcIP/ PrefixLength DotIP/ PrefixLength Proto SrcPurt [DsOPvt] DSOP Check 802.1P C
Security Parental Control Quality of Service Qo5 Queue	Add Enable Renove
QoS Classification	
DNS	
UPoP	
DNS Prany	
IP Tunnel	
Multicast	
Wireless	
Diagnostics	

Para añadir una regla, se debe hacer clic sobre el botón "Add". Más adelante se detalla los campos a configurar en las reglas de clasificación.

Para eliminar reglas, selecciona los *checks "Remove"* correspondientes y haz *click* sobre el botón *"Remove"* de la parte inferior.

El botón "*Enable*" actualiza las colas. Habilita las reglas que tienen el *check* "*Enable*" habilitado y deshabilita las reglas con este *check* deshabilitado. Por tanto, para que los cambios en los *checks* "*Enable*" tengan efecto es necesario pulsar el botón "*Enable*" de la parte inferior.

> C 🕷 🔯	ps://192.168.1.1:8080/main.html	
novista	ne	
	Add Network Traffic Class Rule	
	This screen creates a traffic class rule to classify the ingress traff	ic into a priority queue and optionally mark the DSCP or Ethernet priority of the packet.
evice Info	Click Apply/Save to save and activate the rule,	
vanced Setup	Traffic Class Name:	
ayer2 Interface	Rule Order:	Last 🔻
WAN Service		
LAN	Rule Status:	Enable •
NAT	Specify Classification Oritoria (A black criterion indicates it is	not used for discrification)
Security	Specify classification criteria (A blank criterion indicates it is	not used for classification,
Parental Control	Class Interface:	LAN
Quality of Service		
QoS Queue	Ether Type:	
QoS Classification	Source MAC Address:	
Routing	Source MAC Mask:	
NS	Destination MAC Address:	
IPnP	Destination MAC Mask:	
ONS Proxy		
P Tunnel	Specify Classification Results (A blank value indicates no ope	ration.)
fulticast	Specify Class Oueue (Required):	▼
ireless	- Packets classified into a queue that exit through an interface fo	r which the queue
pice	is not specified to exist, will instead egress to the default queue of	on the interface.
iagnostics		
anagement	Mark Differentiated Service Code Point (DSCP):	•
	Mark 802.1p priority:	T
	 Class non-vlan packets egress to a non-vlan interface will be tai Class vlan packets egress to a non-vlan interface will have the class non-vlan packets egress to vlan interface will be tagged Class vlan packets egress to a vlan interface will be additionally 	gged with VID 0 and the class rule p-bits. oacket p-bits re-marked by the class rule p-bits. No additional vlan tag is added. with the interface VID and the class rule p-bits. tagged with the packet VID, and the class rule p-bits.

Para la generación de una nueva regla de clasificación de tráfico, se deben especificar los siguientes campos:

Сатро	Descripción
Traffic Class Name	Nombre definido por el usuario para la regla de clasificación.
Rule Order	Establecer el número de orden de la regla.
Rule Status	Para crear la regla habilitada o deshabilitada
Class Interface	Interfaz seleccionado
Criterio de la regla de clasificación (En b	lanco indica que ese filtro no se utiliza para la clasificación)
Ethertype	IP (0x0800)
	ARP (0x0806)
	IPv6 (0x86DD)
	PPPoE_DISC (0x8863)
	PPPoE_SES (0x8864)
	8865 (0x8865)
	8866 (0x8866)
	8021Q (0x8100)
Source MAC Address	Dirección de host/red origen

Source MAC Mask	Máscara de red origen
Destination MAC Address	Dirección de host/red destino
Destination MAC Mask	Máscara de red destino
Resultados de la regla de clasificación	(Campo en blanco indica que no se realiza ningún cambio)
Specify Class Queue	 Cola de salida especificada Paquetes que se clasifican en una cola de salida no especificada en el interfaz de salida de la trama, se reasigna a la cola por defecto de dicho interfaz
Mark Differentiated Service Code Point (DSCP)	Valor DSCP establecido en las tramas IP
Mark 802.1p priority	 Prioridad establecida en la tramas con etiqueta VLAN Paquetes salientes sin VLAN por un interfaz sin VLAN serán etiquetados con VLAN 0 y la prioridad correspondiente. Paquetes salientes con VLAN por un interfaz sin VLAN tendrán la prioridad reestablecida por la regla de clasificación, no se añade ninguna etiqueta adicional. Paquetes salientes sin VLAN hacia un interfaz con VLAN será etiquetados con la VLAN del interfaz y con la prioridad de la regla de clasificación correspondiente. Paquetes salientes con VLAN hacia un interfaz de la regla de clasificación de la regla de clasificación de la regla de clasificación

Routing

.

Esta opción permite realizar la configuración de Default Gateway, Static Route, Policy Routing y RIP.

Default Gateway

Seleccione el interfaz WAN como la puerta de enlace por defecto o Default Gateway y haga clic en el botón

"Save/Apply	/".					
Fiber Home Gateway	×	Sector other	straphy in the loss	or or Post & supervised Wanted State		
← → C fi (8)	192.168.1.1:8080/main.html					\$
M movista	ne la					
	Routing Default Gateway Default gateway interface but can have mult	uje WAN interfaces served as system default galervays by	t only one will be used according to the prior	ly with the first being the highest and the last one the lowest pror	Ry if the WAN interface is connected. Priority order can be chan	ped by removing all and adding them back in
Device Info Advanced Setup	again.					
Layer2 Interface WAN Service	Selected Default Gateway Interfaces	Available Routed WAN Interfaces				
LAN		velp0 3 +				
NAT Security		ppp0 1				
Parental Control Quality of Service						
Routing						
Default Gateway	4*					
Policy Routing						
RIP		*				
UPeP						
DNS Proxy IP Tunnel	TODO: JPV6 ********** Select a preferrer	d wan interface as the system default IPv6 gateway-				
Multicast	Internet with Interface Elopol 1 .					
Wireless	Seeces non interace 6/ppp0.1 •					
Diagnostics						
Management				Apply/Save		

Static Route

Esta opción permite configurar rutas estáticas. Haga clic en el botón "*Add*" para añadir una nueva ruta estática. Haga clic en el botón "*Remove*" para eliminar una ruta estática.



Al pulsar el botón "Add" aparece la siguiente imagen:

/ 🗋 Fiber Home Gateway	×	March & - other drop of	And State States in State of Street, St
← → C ♠ 🚯	ps://192.168.1.1:8080/main.html		
M movista	r		
	Routing Static Route Add	k. nateway AND/OR available WAN interface then click "Annly/Save	" to add the entry to the routing table.
Device Info	Enter the destination network address, subnet mas	c, gateway Androik available wAn interface then cick. Apply/Save	to add the endy to the robting table.
Advanced Setup	IP Version:	IPv4	
Layer2 Interface	Destination ID address/profix length:		
WAN Service	beschador te addressyprenx length		
LAN	Interface:		
NAT	Gateway IP Address:		
Security	A sub-state of the state of the		
Parental Control	(optional: metric number should be greater than or Mateix	equal to zero)	
Quality of Service	Metric		
Routing			Apply/Save
Default Gateway			
Static Route			
Policy Routing			
RIP			
DNS			
UPnP			
DNS Proxy			
IP Tunnel			
Multicast			
Wireless			
Voice			
Diagnostics			
Management			

Introduzca la dirección de red de destino, máscara, dirección IP del Gateway, interfaz destino y métrica de la ruta creada. Haga clic en el botón *"Save/Apply"* para salvar la ruta introducida en la tabla de enrutamiento.

Policy Routing

En este apartado se pueden generar políticas de enrutamiento.



Al pulsar el botón "Add" aparece la siguiente pantalla:

/ 🗋 Fiber Home Gateway	×	March & work party and a	surgers where the state of the
← → C fi 🚯	ps://192.168.1.1:8080/main.html		
	Providence		
	Routing Static Route Add		
	Enter the destination network address, subnet mask	., gateway AND/OR available WAN interface then click "Apply/Save"	to add the entry to the routing table.
Device Info		10.4	
Advanced Setup	IP Version:	IPV4	
WAN Service	Destination IP address/prefix length:		
LAN	Interface:	•	
NAT	Gateway IP Address:		
Security			
Parental Control	(optional: metric number should be greater than or	equal to zero)	
Quality of Service	Metric:		
Routing			Apply/Save
Default Gateway			
Static Route			
Policy Routing			
RIP			
DNS			
UPnP			
DNS Proxy			
IP Tunnel			
Multicast			
Wireless			
Voice			
Management			
rianagement			

Para la creación de la política se debe establecer el nombre, puerto físico LAN, dirección IP, interfaz WAN y gateway.

RIP

Para activar RIP, configurar la versión y modo de operación de RIP maque la casilla ve verificación "*Enabled*" para activarlo para al menos un interfaz WAN. Haga clic en el botón "*Save/Apply*".



DNS

DNS Server

Selecciona el interfaz para acceder a los servidores DNS de los interfaces WAN disponibles o configura estáticamente las direcciones IP de los servidores DNS para el sistema. En modo ATM, si se configura un único PVC con IPoA o IPoE, se debe configurar direcciones IP estáticas.

Los interfaces para acceder a los servidores DNS pueden ser múltiples pero sólo se accederá por el interfaz con mayor prioridad.

Para obtener información DNS de un interfaz WAN, marque *"Obtain DNS info from a WAN interface"*, seleccione un interfaz WAN de la lista desplegable. Para DNS estático, marque *"Use the following static DNS IP address"*, e introduzca la dirección IP del DNS primario y la dirección IP del DNS secundario. Haga clic en el botón *"Save/Apply"* para guardar la configuración.

Fiber Home Gateway	
← → C fi Belan	委//192168.11.8080/main.html
M movista	
	DNS Server Configuration
	Seed DMS Server (Indexes Inter-aculate) XMM interfaces CR where XmA interfaces CR where XmA interfaces In ATM mode, if why a ward PR address Att DMS protein is completed. Multi DMS and while we then the interface is completed in the retrest.
Device Info Advanced Setup	
Layer2 Interface	Salact DBIS Sover Interface from available WARI interfaces Extend RM Come Extended RM Comments Extended RM Come Extended RM Comments Ex
LAN	
NAT Sacurity	 veepuid ppp6 1
Parental Control	
Quality of Service Routing	
DNS	
Dynamic DNS	
UPnP DNS Reason	• •
IP Tunnel	
Multicast	Use the following Static DPS IP address
Voice	Printing CR0 Server (2005-05-1-200)
Diagnostics Management	strong land size
	TODN: DVK ***********************************
	8 Oktain 1994 DNS tole form a WIMD interfaces WMN Interface asslerated Gippp0.1.*
	Use the following States Divis DRS address:
	Primary SHid DNS server:
	Secondary IDvG DRS server
	Activity and

Dynamic DNS

El servicio *Dynamic DNS* (DNS dinámico) permite a la dirección IP de su router comportarse como un *hostname* o nombre de dominio, permitiendo al TriWave el acceso desde otros sitios de Internet más fácilmente.



Para añadir un servicio Dynamic DNS, haga clic en el botón "Add". La siguiente pantalla será mostrada:

📕 📄 Fiber Home Gateway	×	Read an and an investigation	Salpha Will Press in Fight & or
← → C fi 🔒 bat	ps :// 192.168.1.1 :8080/m	ain.html	
M movista	or and the second se		
	Add Dynamic DNS		
Device Info	This page allows you to add a	Dynamic DNS address from DynDNS.org or TZO.	
Advanced Setup Layer2 Interface	D-DNS provider	DynDNS.org 🔻	
WAN Service LAN NAT	Hostname Interface	3/veip0.3 T	
Security Parental Control Quality of Service	DynDNS Settings Username		
Routing DNS DNS Server Dynamic DNS	Passivolu		
UPnP DNS Proxy IP Tunnel			Apply/Save
Multicast Wireless Voice			
Diagnostics Management			

Campo	Descripción
D-DNS Provider	Seleccione el proveedor Dynamic DNS de la lista desplegable
Hostname	Introduzca el nombre del servidor DNS dinámico
Interface	Seleccione el interface del desplegable
Username	Introduzca el usuario del servidor DNS dinámico
Password	Introduzca la contraseña del servidor DNS dinámico

UPnP

Marque la casilla de verificación "Enable UPnP" y haga clic en el botón "Apply/Save" para activar el protocolo UPnP.



DNS Proxy

Marque la casilla de verificación "Enable DNS Proxy" y haga clic en el botón "Apply/Save" para activar el protocolo DNS Proxy. Después hay que establecer el nombre del equipo TriWave y nombre del dominio de la red LAN.



IP Tunnel

En este apartado podremos configurar los parámetros para permitir a hosts conectados únicamente a IPv4 ó IPv6 acceder a recursos sólo disponibles utilizando el otro protocolo.

IPv6inIPv4

Aquí podemos configurar un túnel IPv4 para dispositivos IPv6.



Actualmente, TriWave sólo soporta la configuración 6rd:

/ 🗋 Fiber Home Gateway	×		to the local division in the local division of the local divisione
← → C fi 🚱	ps://192.168.1.1:8080/main.html		
M movista	ar		
	IP Tunneling 6in4 Tunnel Configuration		
	Currently, only 6rd configuration is supported.		
Device Info Advanced Setup Layer2 Interface WAN Service LAN NAT Security Parental Control Quality of Service Routing DNS UPnP DNS Proxy IP Tunnel IPv6inIPv4 IDv6inIPv4	Tunnel Name Mechanism: Associated WAN Interface:	6RD V LAN/br0 V	Apply/Save
Multicast Wireless Voice			
Diagnostics			
Management			

Para la configuración hay que establecer el nombre de tunel, y los interfaces WAN y LAN que se van a asociar. Si se opta por configuración manual hay que establcer adicionalmente la longitud de la máscara IPv4, longitud del prefijo 6rd y la dirección IPv4 Relay a la que hay que conectarse.

IPv4inIPv6

Aquí podemos configurar un túnel IPv6 para dispositivos IPv4.



Actualmente, TriWave sólo soporta la configuración DS-Lite:

📄 Fiber Home Gateway 🛛 🗙			
	192.168.1.1:8080/main.html		
M movistar			
	IP Tunneling 4in6 Tunnel Configuration Currently, only DS-Lite configuration is supported.		
Device Info Advanced Setup Layer2 Interface WAN Service LAN NAT Security Parental Control Quality of Service Routing DNS UPnP DNS Proxy IP Tunnel IPv6inIPv4 IPv6inIPv4 IPv6inIPv6 Multicast Wireless Voice Diagnostics Management	Tunnel Name Mechanism: Associated WAN Interface:	DS-Lite	Apply/Save

Para la configuración hay que establecer el nombre de tunel, y los interfaces WAN y LAN que se van a asociar. Si se opta por configuración manual hay que establecer adicionalmente el AFTR (*Address Family Translation Router*).

Multicast

En este apartado se configura los parámetros del protocolo IGMP:

/ 🛅 Fiber Home Gateway		
← ⇒ C fi 🚯	Hps://192.168.1.1:8080/main.html	
M movist	ar	
	Multicast Precedence:	Disable Volume value, higher priority
Device Info Advanced Setup Layer2 Interface	IGMP Configuration Enter IGMP protocol configuration fields if you want modify default valu	ies shown below.
WAN Service	Defails Version	
LAN	Derault Version:	2
Security	Query Interval:	10
Parental Control	Query Response Interval:	10
Quality of Service	Last Member Query Interval:	10
Routing	Robustness Value:	2
DNS	Maximum Multicast Groups:	25
UPnP	Maximum Multicast Data Sources (for IGMPv3):	10
DNS Proxy	Maximum Multicast Group Members:	25
IP Tunnel	Fast Leave Enable:	
Multicast		
Wireless		
Voice	MLD Configuration	
Diagnostics	Enter MLD protocol (IPv6 Multicast) configuration fields if you want mo	dify default values shown below.
Management		
	Default Version:	2
	Query Interval:	15
	Query Response Interval:	10
	Last Member Query Interval:	10
	Robustness Value:	2
	Maximum Multicast Groups:	10
	Maximum Multicast Data Sources (for mldv2):	10
	Maximum Multicast Group Members:	10
	Fast Leave Enable:	

Apply/Save

Сатро	Descripción
Multicast Precedence	Valor del campo "Precedence" que se establecerá en las tramas Multicast
	IGMP Configuration
Default Version	Versión por defecto del protocolo IGMP
Query Interval	Tiempo que ha de transcurrir entre cada <i>Query</i> del equipo. Por defecto, 125 segundos.

Query Response Interval	Tiempo que se inserta en el campo de Tiempo de Respuesta Máximo de los
	mensajes de tipo <i>General Query</i> . Por defecto, 10 segundos.
Last Member Query Interval	Tiempo que se inserta en el campo de Tiempo de Respuesta Máximo de los mensajes de tipo <i>Group-Specific Query</i> . Por defecto, 1 segundo, e indica además el intervalo entre cada una de las <i>Group-Specific Queries</i> .
Robustness Value	Número de veces que un paquete es reenviado. Es útil en redes congestionadas. De 1 a 7. Por defecto, 2.
Maximum Multicast Groups	Número máximo de grupos multicast que se pueden establecer (Por defecto = 25).
Maximum Multicast Data Sources (for IGMPv3)	Número máximo de fuente de datos. Por defecto, 10.
Maximum Multicast Group Members	Número Máximo de miembros en un grupo Multicast: Por defecto, 25.
Fast Leave Enable	Opción que minimiza el tiempo de finalización de un grupo multicast. Si está habilitada esta opción cuando llegue un " <i>Leave</i> " el equipo borra el grupo inmediatamente.
	MLD Configuration (IPv6)
Default Version	MLD Configuration (IPv6) Versión por defecto del protocolo IGMP
Default Version Query Interval	MLD Configuration (IPv6) Versión por defecto del protocolo IGMP Tiempo que ha de transcurrir entre cada "Query" del equipo. Por defecto 125 segundos.
Default Version Query Interval Query Response Interval	MLD Configuration (IPv6)Versión por defecto del protocolo IGMPTiempo que ha de transcurrir entre cada "Query" del equipo. Por defecto125 segundos.Tiempo que se inserta en el campo de Tiempo de Respuesta Máximo de losmensajes de tipo General Query. Por defecto, 10 segundos.
Default Version Query Interval Query Response Interval Last Member Query Interval	MLD Configuration (IPv6)Versión por defecto del protocolo IGMPTiempo que ha de transcurrir entre cada "Query" del equipo. Por defecto 125 segundos.Tiempo que se inserta en el campo de Tiempo de Respuesta Máximo de los mensajes de tipo General Query. Por defecto, 10 segundos.Tiempo que se inserta en el campo de Tiempo de Respuesta Máximo de los mensajes de tipo General Query. Por defecto, 10 segundos.Tiempo que se inserta en el campo de Tiempo de Respuesta Máximo de los mensajes de tipo Group-Specific Query. Por defecto, 1 segundo, e indica además el intervalo entre cada una de las Group-Specific Queries.
Default Version Query Interval Query Response Interval Last Member Query Interval Robustness Value	MLD Configuration (IPv6)Versión por defecto del protocolo IGMPTiempo que ha de transcurrir entre cada "Query" del equipo. Por defecto 125 segundos.Tiempo que se inserta en el campo de Tiempo de Respuesta Máximo de los mensajes de tipo General Query. Por defecto, 10 segundos.Tiempo que se inserta en el campo de Tiempo de Respuesta Máximo de los mensajes de tipo Group-Specific Query. Por defecto, 1 segundo, e indica además el intervalo entre cada una de las Group-Specific Queries.Número de veces que un paquete es reenviado. Es útil en redes congestionadas. De 1 a 7. Por defecto, 2.
Default Version Query Interval Query Response Interval Last Member Query Interval Robustness Value Maximum Multicast Groups	MLD Configuration (IPv6)Versión por defecto del protocolo IGMPTiempo que ha de transcurrir entre cada "Query" del equipo. Por defecto 125 segundos.Tiempo que se inserta en el campo de Tiempo de Respuesta Máximo de los mensajes de tipo General Query. Por defecto, 10 segundos.Tiempo que se inserta en el campo de Tiempo de Respuesta Máximo de los mensajes de tipo General Query. Por defecto, 10 segundos.Tiempo que se inserta en el campo de Tiempo de Respuesta Máximo de los mensajes de tipo Group-Specific Query. Por defecto, 1 segundo, e indica además el intervalo entre cada una de las Group-Specific Queries.Número de veces que un paquete es reenviado. Es útil en redes congestionadas. De 1 a 7. Por defecto, 2.Número máximo de grupos multicast que se pueden establecer. Por defecto, 25.
Default Version Query Interval Query Response Interval Last Member Query Interval Robustness Value Maximum Multicast Groups Maximum Multicast Data Sources (for IGMPv3)	MLD Configuration (IPv6)Versión por defecto del protocolo IGMPTiempo que ha de transcurrir entre cada "Query" del equipo. Por defecto 125 segundos.Tiempo que se inserta en el campo de Tiempo de Respuesta Máximo de los mensajes de tipo General Query. Por defecto, 10 segundos.Tiempo que se inserta en el campo de Tiempo de Respuesta Máximo de los mensajes de tipo Group-Specific Query. Por defecto, 1 segundo, e indica además el intervalo entre cada una de las Group-Specific Queries.Número de veces que un paquete es reenviado. Es útil en redes congestionadas. De 1 a 7. Por defecto, 2.Número máximo de grupos multicast que se pueden establecer. Por defecto, 25.Número máximo de fuente de datos. Por defecto, 10.

Members	
Fast Leave Enable	Opción que minimiza el tiempo de finalización de un grupo multicast. Si
	está habilitada esta opción cuando llegue un "Leave" el equipo borra el
	grupo inmediatamente.

Wireless

El menú *Wireless* facilita acceso a las opciones de configuración del enlace inalámbrico, como se muestra a continuación.

Basic

La opción "*Basic*" permite configurar los parámetros básicos del interfaz inalámbrico (WLAN). Puede activar o desactivar el interfaz inalámbrico, ocultar la red a escaneos actives, configurar el nombre de red inalámbrica (también conocido como SSID) y restringir el canal a los requerimientos de configuración de país.

🖉 🗋 Fiber Home Gateway 🛛 🗙	0								And a second sec
← → C fi (k batps:/	/192.168.	1.1:8080/main.html							
M movistar									
	Wireless - This page a Click "Apply	• Basic llows you to configure basic features of t /Save" to configure the basic wireless op	he wireles tions.	s LAN inte	rface. You c	an enable	or disabl	le the wi	eless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements.
Advanced Setup Wireless Basic Socurity MAC Filter Wireless Bridge Advanced Station Info Voice Diagnostics Management	En En En En En Di Di En SSID: Country: Country: Country:	able Wireless able Wireless bitspot2.0 de Access Point ents Isolation sable WMM Advertise able Wireless Multicast Forwarding (WM MOVISTAR_DEAB 76:30:580:10:6EA9 76:30:580:10:6EA9 5PAIN gRev 0 s 32 s 32	F)				·		
	Wireless -	Guest/Virtual Access Points: SSID wl0_Gwest1 wl0_Gwest2 wl0_Guest3	Hidden	Isolate Clients	Disable WMM Advertise	Enable WMF	Max Clients 16 16	BSSID N/A N/A	
	Apply/Sa	ve							

Haga clic en el botón "Save/Apply" para aplicar las opciones inalámbricas seleccionadas.

Consulte la siguiente tabla para la descripción de cada opción.

Campo	Descripción
Enable Wireless	Activa o desactiva el interfaz inalámbrico. Cuando está marcada, las opciones de configuración básicas serán mostradas.
Enable Wireless Hotspot2.0	Si está activo mejora las prestaciones de los dispositivos Wi-Fi para descubrir y conectarse a nuestro equipo.
Hide Access Point	Si está activo, protege el punto de acceso de la detección por escaneo inalámbrico. Por ejemplo: Para chequear el estado del punto de acceso en Windows XP, abra "Conexiones de Red" desde el menú Inicio y seleccione "Ver conexiones de red disponibles". Si el punto de acceso está oculto, no será mostrado en la lista. Para conectar con un punto de acceso oculto, la estación debe añadir el punto de acceso de forma manual a la configuración inalámbrica.
Clients Isolation	Cuando está activado, impide que los PCs asociados a la red inalámbrica sean vistos desde "Mis sitios de Red" o desde redes vecinas. También, impide que un cliente inalámbrico pueda comunicarse con otro cliente inalámbrico.
Disable WMM Advertise	Detiene al router de publicar la funcionalidad WMM o Wireless Multimedia, la cual facilita la calidad de servicio básica para aplicaciones en tiempo real (ej. VoIP, Video).
Enable Wireless Multicast Forwarding (WMF)	Si está activado permite al router reencaminar paquetes a otras redes dónde otros dispositivos multicast están activos y escuchando.
SSID (1-32 caracteres)	Configura el nombre de la red inalámbrica. El SSID significa <i>Service Set</i> <i>IDentifier</i> . Todas las estaciones deben configurado correctamente el SSID para acceder a la WLAN. Si el SSID no es correcto, el usuario no tiene garantizado el acceso.
BSSID	El BSSID es un identificado de 48 bit usado para identificar un BBS en particular (<i>Basic Service Set</i>) dentro de un área. En infraestructuras de redes BSS, el BSSID es la dirección MAC del punto de acceso; y en BSS independientes o red ad hoc, el BSSID es generado aleatoriamente.
Country	Una lista desplegable permite seleccionar la configuración específica del país seleccionado. Leyes locales regulan el límite y rango de canales, como por ejemplo: US= worldwide, Japan=1-14, Jordan= 10-13, Israel= 1-13
Max Clients	El número máximos de clientes que pueden acceder al equipo.

Wireless - Guest /El TriWave soporta múltiples SSID llamados Guest SSIDs o Virtual AccessVirtual Access PointsPoints (punto de accesos virtuales). Para activar uno o más de un GuestSSIDs marque la casilla de verificación en la columna "Enabled". Para
ocultar un SSID marque la casilla de verificación en la columna "Hidden".
Haga lo mismo para "Isolate Clients" y "Disable WMM Advertise". Para una
descripción de estas dos funcionalidades, consulte las filas anteriores de
los campos "Clients Isolation" y "Disable WMM Advertise". De igual modo,
para "Max Clients" y "BSSID", consulte las entradas coincidentes en esta
tabla.

Nota: Host inalámbrico remoto no puede escanear Guest SSIDs.

Security

La siguiente pantalla aparecerá cuando es seleccionado "**Wireless Security**". Las opciones mostradas aquí permiten configurar los parámetros de seguridad del interfaz inalámbrico.

/ 🗋 Fiber Home Gateway 🛛 🗙		The second design of the secon
← → C A Steps:	//192.168.1.1:8080/main	html
M movistar		
Device Info Advanced Setup Wireless	Wireless Security This page allows you to configure You may setup configuration man OR through WiFi Protctad Setup(WPS Note: When both STA PIN and Au	security features of the wireless LAN interface. ually thorized MAC are empty, PBC is used. If Hide Access Point enabled or Mac filter list is empty with "allow" chosen, WPS2 will be disabled
Basic Security MAC Filter Wireless Bridge	WPS Setup Enable WPS	Enabled v
Advanced Station Info Voice Diagnostics	Add Client (This feature is av	ailable only when WPA-PSK(WPS1), WPA2 PSK or OPEN mode is configured) Image: Use STA PIN Use AP PIN Add Enrollee Help Help
rianagement	Set Authorized Station MA	Configured
	Setup AP (Configure all securi	ty settings with an external registar)
	Device PIN	93423700 Help
	Manual Setup AP You can set the network authentic specify whether a network key is r Click "Apply/Save" when done.	ation method, selecting data encryption, equired to authenticate to this wireless network and specify the encryption strength.
	Select SSID:	MOVISTAR_0EA8 V
	Network Authentication:	WPA2 -PSK T
	WPA/WAPI passphrase: WPA Group Rekey Interval: WPA/WAPI Encryption: WEP Encryption:	0 Click here to display 0 AES Disabled
		Apply/Save

Haga clic en el botón "Save/Apply" para implementar los nuevos parámetros de configuración.

WIRELESS SECURITY

Los parámetros de seguridad inalámbrica pueden ser configurados manualmente o a través de WI-FI *Protected Setup* (WPS). El método WPS configura los parámetros de seguridad automáticamente (consultar apartado 6.2.1) mientras que el método *Manual Setup* requiere que el usuario configures estos parámetros usando el interfaz de usuario Web. Ver siguiente tabla.

Seleccionar SSID:

Seleccionar el nombre de red inalámbrica de la lista desplegable. Todas las estaciones deben tener configurado correctamente el SSID para acceder a la WLAN. Si el SSID no es correcto, el usuario no tiene garantizado el acceso.

Network Authentication:

Esta opción especifica si algún protocolo se utiliza para la autenticación de la red inalámbrica. Si la autenticación de red está configurada como *Open*, entonces no existe autenticación. A pesar de ello, la identidad del cliente es todavía verificada.

Los posibles métodos de autenticación son: Open (sin autenticación), Shared, 802.1x, WPA, WPA-PSK, WPA2, WPA2-PSK, Mixed WPA2/WPA, Mixed WPA2/WPA-PSK.

Cada tipo de autenticación tiene sus propios parámetros. Por ejemplo, seleccionando autenticación 802.1X se deberá especificar la dirección IP del servidor Radius, puerto y campo clave.

Network Authentication:	802.1X	~
RADIUS Server IP Address:	0.0.0.0	
RADIUS Port:	1812	
RADIUS Key:		

WEP Encryption

Esta opción especifica si los datos enviados en una red están encriptados. La misma clave de red es usada para la encriptación de datos y autenticación de red. Cuatro claves de red pueden ser definidas aunque una única puede ser usada al mismo tiempo. Use la lista desplegable **"Current Network Key"** para seleccionar la clave red adecuada.

Las opciones de seguridad incluye autenticación y encriptación basada en el algoritmo Wired Equivalent Privacy (WEP). WEP es un servicio de seguridad configurable usado para proteger redes 802.11 de accesos no autorizados, tales como escucha; en este caso, la captura de tráfico inalámbrico. Cuando la encriptación de datos está activada, la clave secreta compartida de encriptación es generada y usada por la estación origen y la estación destino para modificar a otro rango de bits, evitando así la divulgación a espías.

Bajo autenticación de clave compartida, cada estación inalámbrica asume tener un receptor de clave compartido sobre un canal seguro que es independiente del calan de comunicaciones de red inalámbrica.

Encryption Strength

Esta lista desplegable se mostrará cuando la encriptación WEP este habilitada. La longitud de la clave es proporcional al número de bits binarios que componen la clave.

Esto significa que las claves con mayor número de bit tienen un mayor grado de seguridad y son considerablemente más difíciles de averiguar.

El tamaño de encriptación puede ser configurado a 64 bit o a 128 bits. Una clave de 64 bit es equivalente a 5 caracteres ASCII o diez números hexadecimales. Una clave de 128 bits contiene 13 caracteres ASCII o 26 números hexadecimales. Cada clave contiene una cabecera de 24 bits (un iniciador de vector) que permite la decodificación de múltiples cadenas de datos encriptados.

MAC Filter

Esta opción permite acceder al router realizar una gestión de restricciones basada en direcciones MAC. Para añadir un filtro de dirección MAC, haga clic en el botón "**Add**" mostrado a continuación. Para eliminar un filtro, seleccione la dirección MAC de la tabla de direcciones MAC mostrada a continuación y haga clic en el botón "**Remove**".

M movistar	
	Wireless MAC Filter
Device Info	Select SSID: MOVISTAR_1341 •
Advanced Setup	
Wireless	MAC Restrict Mode: 🔘 Dirabled 🔘 Allow 🔘 Dany Note: If 'allow' is choosed and mac filter is empty. WP5 will be disabled
Basic	
Security	
MAC Filter	MAC Address Remove
Wireless Bridge	<u> </u>
Advanced	
Station Info	Add Remove
Voice	
Diagnostics	
Management	

Campo	Descripción
Select SSID	Selecciona el nombre de red inalámbrico de la lista desplegable. SSID significa <i>Service Set Identifier</i> . Todas las estaciones deben estar configuradas con el SSID correcto para acceder a la WLA. Si el SSID no es correcto, el cliente no tiene garantizado el acceso.
MAC Restrict Mode	 Disabled: Filtrado MAC desactivado. Allow: Acceso permitido a las direcciones MAC especificadas. Deny: Acceso restringido a las direcciones MAC especificadas.

MAC Address	Enumera las direcciones MAC sujetas al modo de restricciones MAC. Se
	puede añadir un máximo de 60 direcciones MAC. Cada dispositivo de
	RED tienen una única dirección MAC de 48 bit. Normalmente mostrada
	como xx.xx.xx.xx.xx.xx, donde xx es un número hexadecimal.

Después de pulsar sobre el botón "*Add*", la siguiente pantalla aparecerá. Introduzca la dirección MAC en el campo facilitado y haga clic en el botón "*Save/Apply*".

Wireless Bridge

Esta opción permite la configuración de la funcionalidad Bridge inalámbrico del interfaz WLAN. Consulte la tabla inferior para conocer más detalles de las distintas opciones.

Fiber Home Gateway	×	
← → C n Beber	://192.168.1.1:8080/main.htm	
M movistar		
	Wireless - Bridge	
Device Info Advanced Setup Wireless Basic	This page allows you to configure wire Bridger will be granted acress. Cick, "Refersh 'to spatiat the remote b Click. "Apply/Seve" to configure the wire	bridge features of the viviless LAN interface. Select Disabled in Bridge Restrict which disables inveless bridge restriction. Any wiveless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables invelees bridge restriction. Only these bridges selected in Remote as Walk for few seconds to update
Security	Bridge Restrict:	Enabled
Mirekans Binkye Advanced Station Binkye Volce Diagnestics Hamgement	Remate Bridges MAC Address	
		[Ashmah] [Ashmah]

Haga clic en el botón "Save/Apply" para salvar y aplicar los parámetros de la nueva configuración.

ge, lo que indica
. Seleccionando
bridge. Sólo los
<i>3ridges"</i>) tendrán
ualizar la lista de
bri Brid Jali

Advanced

El submenú "Advanced" permite configurar las prestaciones avanzadas del interfaz inalámbrico. Puede seleccionar un canal en particular con el que operar, aplicar una velocidad en particular para forzar el rango de transmisión, configurar el umbral de fragmentación, configurar el umbral RTS, configurar *wake interval* para clientes en modo ahorro de energía o *power-save*, configurar el *beacon interval* para el punto de acceso, configurar el modo *XPress* y configurar si el preámbulo usado es corto o largo. Haga clic en el botón "*Save/Apply*" para configurar las nuevas opciones inalámbricas avanzadas.



Campo	Descripción
Band	Configure 2.4 GHz para compatibilidad con dispositivos IEEE 802.11x estándar. La
	nueva enmienda permite a los dispositivos 802.11n ser compatibles y coexistir en
	la misma red inalámbrica con dispositivos de velocidades 802.11x inferiores. IEEE
	802.11g iguala el rango de datos en la frecuencia 2,4 GHz con dispositivos
	802.11a, los cuales tienen un rango de 54Mbps en la frecuencia de 5GHz. (IEEE
	802.11a tiene otras diferencias comparadas con IEEE 802.11b y g, como la
	cantidad de canales ofrecidos).
Channel	Seleccione un canal de la lista
Auto Channel Timer (min)	La auto búsqueda de canales temporizado en minutes. ("0", para deshabilitar)

802.11n/EWC	Un equipo configurado con los parámetros de estándar de interoperabilidad en
	IEEE 802.11n Draft 2.0 y Enhanced Wireless Consortium (EWC)
Bandwidth	Seleccione la banda de frecuencia de 20GHz o 40GHz. La banda de frecuencia de
	40GHz usa dos bandas adyacentes de 20 GHz para incrementar el Throughput de
	datos.
Control Sideband	Seleccionar sideband alta o baja cuando está en modo 40GHz.
802.11n Rate	Configurar el rango de transmisión físico (PHY).
802.11n Protection	Off para <i>throughput</i> maximizado.
	Auto para mayor seguridad.
Support 802.11n Client Only	Off para permitir a clientes 802.11b/g acceder al router.
	On para prohibir a clientes 802.11b/g acceder al router.
RIFS Advertisement	Es una característica del 802.11n que mejora las prestaciones reduciendo los
	intervalos entre transmisiones OFDM.
	Off para deshabilitarlo.
	Auto para activarlo.
OBSS Coexistence	Activa o desactiva la coexistencia entre 20-40MHz en redes de área local
	inalámbricas.
Rx Chain Power Save	Si habilitas está característica, apagas una de las cadenas de recepción y de esta
	manera ahorrar potencia.
Rx Chain Power Save Quiet	Número de segundos que el tráfico debe estar por debajo del valor PPS antes de
Time	activar la característica "Rx Chain Power Save"
Rx Chain Power Save PPS	Número máximo de paquetes por segundo que puede procesar el interfaz WLAN
	durante el "Quiet Time" descrito en el campo previo, antes que el "Rx Chain
	PowerSave" se active.
54g [™] Rate	La lista desplegable especifica los siguientes rangos fijos: Auto: Default. Usa el
	rango de datos de 11 Mbps cuando es necesario. Rangos fijos de 1 Mbps, 2Mbps,
	5.5Mbps, o 11Mbps. Los parámetros apropiados dependen de la calidad de la
	señal inalámbrica.
Multicast Rate	Parámetros para el rango de paquetes multicast transmitidos (1 -54 Mbps)
Basic Rate	Configuración de rango básico de transmisión.
Fragmentation Threshold	Un umbral, especificado en bytes, que determina qué paquetes se fragmentarán
	y a qué tamaño. En una WLAN 802.11, los paquetes que exceden el umbral de

fragmentación serán fragmentados, por ejemplo, divididos en, unidades más pequeñas adecuadas al tamaño del circuito. Lo paquetes más pequeños que el umbral de fragmentación especificado no serán fragmentados. Introduzca el valor entre 256 y 2346. Si tiene un alto índice de error de paquetes, trate de aumentar ligeramente el umbral de fragmentación. La configuración del valor debe permanecer entre los parámetros por defecto configurados a 2346. Configurar los parámetros de fragmentación demasiado bajos puede crear problemas de prestaciones.

RTS ThresholdSolicitud a enviar, cuando está configurado en bytes, especifica el tamaño de
paquete más allá del que la tarjeta inalámbrica invoca en su mecanismo RTS/CTS.
Los paquetes que excedan el umbral RTS especificado hacen funcionar el
mecanismo RTS/CTS. La tarjeta transmite paquetes más pequeños sin utilizar
RTS/CTS. El valor por defecto es 2347 (longitud máxima) desactiva el umbral RTS.

DTIM Interval Delivery Traffic Indication Message (DTIM) es también conocido como el Beacon Rate. El rango permitido es un valor entre 1 y 65536. Un DTIM es un contador que informa a los clientes de la próxima ventana para escuchar los mensajes broadcast y multicast. Cuando el AP ha amortiguado el impacto de los mensajes broadcast y multicast para los clientes asociados, envía el próximo DTIM con un valor de intervalo de un DTIM. Los puntos de acceso clientes escuchan el beacon y empiezan a recibir los mensajes broadcast y multicast. Por defecto es "1".

Beacon Interval La cantidad de tiempo entre transmisiones de *beacon* en milisegundos. Por defecto es 100ms y el rango permitido es de 1 a 65535. La transmisión de *beacon* identifica la presencia del punto de acceso. Por defecto, los dispositivos de red pasivos escanean todas las frecuencias de canales escuchando los siguientes puntos desde donde acceder. Antes de que una estación entre en modo de ahorro de energía o *power-saving*, la estación necesita el intervalo de *beacon* para conocer cuándo debe volver a escuchar para recibir el *beacon* (y aprender si existen tramas en el buffer del punto de acceso)

Global Max Clients	El número máximo número de clientes que pueden conectarse al router.
Xpress [™] Technology	Xpress Technology cumple con el borrador de especificaciones de los estándares planteados por los fabricantes inalámbricos.
Transmit Power	Fija la potencia de salida (por porcentaje) deseado.
WMM (Wi-Fi Multimedia)	La tecnología para mantener la prioridad de aplicaciones de voz, audio y video en redes inalámbricas. Permite a los servicios multimedia tener mavor prioridad.
WMM No Acknowledgement	Referido a la política de conocimiento a nivel MAC. Activando un "no acuse" de
------------------------	--
	recibo que puede resultar en una transferencia de datos más eficiente pero más
	propenso a errores en entornos con ruido en radio frecuencia.
WMM APSD	Entrega de power save automático. Este método permite ahorrar energía.

Station Info

Esta sección muestra el modo de autenticación de las estaciones inalámbricas y su estado. Haga clic en el botón *Refresh* para actualizar la lista de estaciones asociadas a la WLAN.

🖡 🖹 Fiber Home Gateway	×	Statement of the local division of the local	Station of Station	And in case of the local division of the loc	Marriel Manager
← → C 🕯 🔒 b#ps	://192.168.1.1:8080/ma	in.html			
	Wireless Authenticated S	tations			
Device Info Advanced Setup Wireless Basic Security MAC Filter Wireless Bridge Advanced Station Info Voice Disconcetics	This page shows authenticated MAC Associated Author	wireless stations and their status.			Refresh
Management					

Campo	Descripción
MAC	Lista de direcciones MAC de todas las estaciones
Associated	Lista de todas las estaciones que están asociadas al punto de acceso, mostrando el tiempo de conexión y paquetes emitidos y recibidos por cada una de las estaciones. Si la estación es parada durante mucho tiempo, es eliminada de la lista.
Authorized	Lista los dispositivos con acceso autorizado.
SSID	Muestra los SSID del router a los que las estaciones están conectados.
Interface	Muestra las interfaces del router a las que las estaciones están conectadas.

Voice

En este apartado se podrá visualizar y configurar todos parámetros relativos a la voz del TriWave

SIP Basic Setting

En la pestaña de parámetros globales aparece la siguiente figura dónde debemos elegir el interfaz, IPv4 o IPv6, iniciar o detener el cliente SIP y poder restaurar los valores por defecto.

/ 🗋 Fiber Home Gateway 🛛 🗙		A COLUMN TWO IS NOT
	//192.168.1.1:8080/main.html	
M movistar		
Device Info Advanced Setup Wireless Voice SIP Basic Setting SIP Advanced Setting Diagnostics Management	Global parameters Service Provider 0 Global parameters Bound Interface Name: veip0.3 ▼ IP Address Family: IPv4 ▼ NOTE: Interface and address family changes require the SIP client to be stopped and then started to take effect	Start SIP client Stop SIP client Restore default setting Apply

Si seleccionamos la pestaña "Service Provider 0" aparace la siguiente pantalla:

SIP Basic Setting



En esta pantalla tenemos los siguientes parámetros configurables:

Campo	Descripción
Locale selection	Especifica qué características locales se están usando. En esta versión del TriWave sólo está presente la opción ESP-SPAIN.
SIP domain name	Especifica el nombre de dominio utilizado para los mensajes SIP salientes.
Voip Dialplan Setting	Especifica el <i>DialPlan</i> que debe coincidir para todas las llamadas VoIP salientes.

SIP Proxy	
SIP Proxy	Nombre o dirección IP del SIP Proxy
SIP Proxy port	Puerto del servidor del SIP Proxy
SIP Outbound Proxy	
SIP Outbound Proxy	Nombre o dirección IP del SIP Outbound Proxy
SIP Outbound Proxy port	Puerto del servidor del SIP Outbound Proxy
SIP Registrar	
SIP Registrar	Nombre o dirección IP del SIP registrar
SIP Registrar port	Puerto del servidor del SIP registrar
SIP Account	
SIP Account	Número de cuenta SIP (0 y 1)
Account Enabled	Especifica si esta cuenta está habilitada o no.
Extension	Especifica la extensión o número de teléfono de esta cuenta. Este valor es el ID del usuario en un SIP URI. Por ejemplo, si la extensión es "123456", entonces el SIP URI en la cabecera en todos los mensajes salientes será: From: "NOMBRE" <sip:123456@xxx></sip:123456@xxx>
Display name	Especifica el nombre para esta cuenta. Este valor es el nombre que aparecerá en el SIP URI. Por ejemplo, si el nombre es "ALICIA", entonces la cabecera de todos los mensajes salientes será: From: "ALICIA" <sip:123456@xxx></sip:123456@xxx>
Authentication name	Especifica el nombre utilizado en todas las sesiones de autenticación SIP
Password	Especifica el password utilizado en todas las sesiones de autenticación SIP
Preferred ptime	Especifica el intervalo entre paquetes en ms para el códec utilizado. Valores válidos son 10, 20 y 30 ms.
Preferred codec N	Especifica el orden y tipo de códec que son anunciados en los campos SDP que son enviados en las negociaciones SIP. <i>Preferred codec</i> "1", será el prioritario.

SIP Advanced Setting

Account of Account in Account in Account in Account in Activation Instructions Internet Internet <t< th=""><th></th><th></th><th></th><th></th><th></th></t<>					
P Time in the manufact of the	novistar				
P Ting is attring P P Ting is attring is attri					
P Enable SIP Call Features factors Account 0 Account 1 When enabled, dal "51 to activate factors Call vanito 0 0 When enabled, dal "51 to activate 0 factors Finance 0 0 When enabled, dal "51 to activate 0 0 factors 0 0 When enabled, dal "51 to activate 0 0 0 factors 0 0 When enabled, dal "71 to activate 75 to deactivate factors 0 0 When enabled, dal "71 to activate 0 0 Call barring pin 0 When enabled, dal "71 to activate 0 0 0 Call barring digit map 0 When enabled, dal "71 to activate 0 </th <th></th> <th>Global parameters Service P</th> <th>rovider 0</th> <th></th> <th></th>		Global parameters Service P	rovider 0		
P Enabled SIP Call Features Tender Account 0 Account 3 Activation Instructions Feature 0 0 When enabled, dui "12 to activate, "05 to doctivate Call forward unconditionally 0 When enabled, dui "12 to activate, "75 to doctivate Forward unconditionally 0 When enabled, dui "12 to activate, "75 to doctivate Call forward unconditionally 0 When enabled, dui "12 to activate, "75 to doctivate Call barring digit map 0 When enabled, dui "12 to activate, "75 to doctivate/activate		Voice SIP Advanced conf	iguration		
P Account 0 Account 1 Activation Instructions Gall waiting Image: Control Contend Contrecon Control Contrel Conterve Control Contro Contend Con				Enab	ed SID Call Features
ing Image: Call forwarding number Image: Call forwarding number if setting Image: Call forwarding number Image: Call forwarding number if orward nuconditionality Image: Call forwarding number Image: Call forwarding number if orward nuconditionality Image: Call forwarding number Image: Call forwarding number if orward no "nuog" Image: Call forwarding number Image: Call forwarding number if all barring pin 9999 9999 Image: Call forwarding number if all barring digit map Image: Call forwarding number Image: Call forwarding number Image: Call forwarding number if all barring digit map Image: Call forwarding number Image: Call forwarding number Image: Call forwarding number if all barring digit map Image: Call forwarding number Image: Call forwarding number Image: Call forwarding number if all barring digit map Image: Call forwarding number Image: Call forwarding number Image: Call forwarding number if all barring digit map Image: Call forwarding number Image: Call forwarding number Image: Call forwarding number if all barring digit map Image: Call forwarding number Image: Call forwarding number Image: Call forwarding number Image: Call forwarding	ıp	Feature	Account 0	Account 1	Activation Instructions
ing Call forward in number Image: Call forward in conditionally Image: Call forward in conditionally is exting Forward in "base?" Image: Call forward in the forward in th		Call waiting			When enabled, dial *61 to activate, *60 to deactivate
5 stting Forward unconditionally Image: String and String an	tting	Call forwarding number			
Forward on "busy" When enabled, dal "21 to activate, "75 to deactivate Forward on "no answer" When enabled, dal "21 to activate, "75 to deactivate Call barring When enabled, dal "21 to activate, "75 to deactivate/activ	d Setting	Forward unconditionally			When enabled, dial *71 to activate, *75 to deactivate
Forward on "no answer" Image: Status in the status in		Forward on "busy"			When enabled, dial *71 to activate, *75 to deactivate
Call barring Image: Strate of the strate		Forward on "no answer"			When enabled, dial *71 to activate, *75 to deactivate
Call barring pin 999 999		Call barring			When enabled, dial *85[PIN]0/*85[PIN]1/*85[PIN]2 to deactivate/activate/activate per digit
Call barring digit map Warm line Warm line Warm line number Aronymous call blocking Anonymous call blocking Warm line number Anonymous call blocking Warm line number Anonymous calling Image: State of the state		Call barring pin	9999	9999	
Warn line When enabled, dial "78 to activate, "79 to deactivate Warn line number When enabled, dial "80 to activate, "81 to deactivate Anonymous calling When enabled, dial "80 to activate, "81 to deactivate Anonymous calling When enabled, dial "86 to activate, "81 to deactivate DND When enabled, dial "86 to activate, "87 to deactivate Enable T38 support When enabled, dial "86 to activate, "87 to deactivate Enable V18 support Provide the enabled, dial "86 to activate, "87 to deactivate Enable T38 support Provide the enabled, dial "86 to activate, "87 to deactivate Enable V18 support Provide the enabled, dial "86 to activate, "87 to deactivate DSCP for SIP1: Provide the enabled, dial "86 to activate, "87 to deactivate DSCP for SIP1: Provide the enabled, dial "86 to activate, "87 to deactivate DSCP for SIP1: Provide the enabled, dial "86 to activate, "87 to deactivate DSCP for SIP1: Provide the enabled, dial "86 to activate, "87 to deactivate SIP Tansport protocol": UDP V SIP Tansport protocol": D60.00 Music Server": 00.00 Orderence URI1': 00.00 Conference URI1': 00.00 Conference URI1': 00		Call barring digit map			
Warm line number		Warm line			When enabled, dial *78 to activate, *79 to deactivate
Anonymous call blocking Anonymous calling Monoymous calling Image: transmitting transmitti		Warm line number			
Anonymous calling Image: Construct and C		Anonymous call blocking			When enabled, dial *80 to activate, *81 to deactivate
Image: Internet and the second and		Anonymous calling			When enabled, dial *82 to activate for current call
Findle T38 support Enable T38 support Registration Expire Timeout* 0		DND			When excluded did 200 to reliance 207 to denotion to
Enable T38 support					
Image: Structure struct 0 Registration Expire Timeout* 0 Registration Reby Interval 20 DSCP for SIP*: Image: Structure stru		Enable T38 support			
Image: Strip interval 0 DSCP for SIP*: Image: Strip interval DSCP for RTP*: Image: Strip interval DSCP for RTP*: Image: Strip interval Dtmf Relay setting*: Image: Strip interval SIP Transport protocol*: UDP Image: Strip interval Image: Strip Configuration*: Disabled Image: Strip interval Image: Strip interval 0					
Registration Expire Timeout* 0 Registration Retry Interval 20 DSCP for SIP*: Image: Single Singl		🗹 Enable V18 support			
Registration Reby Interval 20 DSCP for SIP*: Image: Sinterval DSCP for RTP*: Image: Sinterval Dtmf Relay setting*: Image: Sinterval Hook Flash Relay setting*: None Image: Sinterval SIP Transport protocol*: UDP Image: Sinterval SRTP Configuration*: Disabled Image: Sinterval Image: Server port*: 0 Conference URI*: Conference URI*: Conference URI*: Image: Sinterval		Registration Expire Timeout*	0		
DSCP for SIP*: DSCP for SIP*: DSCP for RTP*: Dtmf Relay setting*: Hook Flash Relay setting*: None Hook Flash Relay setting*: UDP SIP Transport protocol*: UDP SIP Transport protocol*: UDP SIP Transport protocol*: Disabled Configuration*: Conference URI*: Conference Obtion*: Local		Registration Retry Interval	20	_	
DSCP for RTP*: Dtmf Relay setting*: Hook Flash Relay setting*: SIP Transport protocol*: UDP ▼ SRTP Configuration*: Enable SIP tag matching* (Uncheck for Vonage Interop). Music Server*: Music Server*: Conference UR1*: Conference UR1*: C					
Dtmf Relay setting*: InBand ▼ Hook Flash Relay setting*: None ▼ SIP Transport protocol*: UDP ▼ SRTP Configuration*: Disabled ▼		DSCP for SIP*:		•	
Hook Flash Relay setting*: None SIP Transport protocol*: UDP SRTP Configuration*: Disabled SRTP Configuration*: Disabled Conference URI*: Conference UR		DSCP for SIP*: DSCP for RTP*:		•	
SIP Transport protocol*: UDP SRTP Configuration*: Disabled Enable SIP tag matching* (Uncheck for Vonage Interop). Music Server*: 0.0.0.0 Music Server*: 0.0.0.0 Conference URI*: 0 Co		DSCP for SIP*: DSCP for RTP*: Dtmf Relay setting*:	InBand V	•	
SRTP Configuration*: Disabled ▼ Image: Enable SIP tag matching* (Uncheck for Vonage Interop). Music Server*: 0.0.0.0 Music Server port*: 0 Conference URI*: 0		DSCP for SIP*; DSCP for RTP*; Dtmf Relay setting*; Hook Flash Relay setting*;	InBand ▼ None ▼	•	
Conference UR1*: Confe		DSCP for SIP"; DSCP for RTP"; Dtmf Relay setting"; Hook Flash Relay setting"; SIP Transport protocol";	InBand V None V UDP V	V V	
Music Server*: 0.0.0.0 Music Server port*: 0 Conference URI*:		DSCP for SIP*: DSCP for RTP*: Dtmf Relay setting*: Hook Flash Relay setting*: SIP Transport protocol*: SRTP Configuration*:	InBand V None V UDP V Disabled V	Y	
Music Server port*: 0 Conference URI*: Conference URI*:		DSCP for SIP*: DSCP for RTP*: Dtmf Relay setting*: Hook Flash Relay setting*: SIP Transport protocol*: SRTP Configuration*: C Enable SIP tag matching	InBand V None V UDP V Disabled V	T	
Conference URI*:		DSCP for SIP*: DSCP for RTP*: Dtmf Relay setting*: Hook Flash Relay setting*: SIP Transport protocol*: SRTP Configuration*: C Enable SIP tag matching Music Sanaer*:	InBand V None V UDP V Disabled V	▼ ▼	
		DSCP for SIP*: DSCP for RTP*: Dtmf Relay setting*: Hook Flash Relay setting*: SIP Transport protocol*: SRTP Configuration*: Configuration*: Music Server*: Music Server*: Music Server port*:	InBand V None V Disabled V (Uncheck for Vonage I 0.0.0.0 0	T	
		DSCP for SIP*: DSCP for RTP*: Dtmf Relay setting*: Hook Flash Relay setting*: SIP Transport protocol*: SRTP Configuration*: Configuration*: Music Server*: Music Server port*: Configure UPTb	InBand V None V Disabled V bisabled V b* (Uncheck for Vonage I 0.0.0.0 0	T Interop).	

Campo	Descripción
Call waiting	Activa la llamada en espera en esta cuenta
Call forwarding number	Especifica el número de teléfono al que se desviarán las llamadas cuando el desvío de llamadas este habilitado
Forward unconditionally	Activa incondicionalmente el desvío de llamadas en esta cuenta
Forward on "busy"	Activa el desvío de llamadas cuando la cuenta está ocupada
Forward on "no answer"	Activa el desvío de llamadas cuando no hay respuesta en esta cuenta
Call barring	Activa la característica de bloqueo de llamadas salientes

Call barring pin	Especifica el PIN a utilizar cuando activamos el bloqueo de llamadas
	desde el terminal.
Call barring digit map	Especifica los números de teléfono que serán restringidos y serán
	comparados en cada ocasión para determinar si aplica el bloqueo de
	llamadas.
Warm line	Habilita la opción de configurar un número de teléfono para soporte
Warm line number	Especifica el número de teléfono de soporte.
Anonymous call blocking	Activa el bloqueo de llamadas entrantes anónimas.
Anomymous calling	Evita enviar información CLID (Calling Line Identification) en las
	llamadas salientes desde esta cuenta
DND	Activa la característica "No molestar" en esta cuenta.
Enable T38 Support	Habilita esta característica.
Enable V18 Support	Habilita esta característica.
Registration Expire Timeout	Especifica el timeout para el registro SIP
Registration Retry Interval	Especifica el intervalo de reintentos para el registro SIP
DSCP for SIP	Valor DSCP para los paquetes SIP salientes
DSCP for RTP	Valor DSCP para los paquetes RTP salientes.
Dtmf Relay Setting	Especifica el método a utilizar cuándo se transmiten los dígitos DTMF.
	Los posibles valores son:
	- SIPInfo: vía paquetes SIP INFO.
	- In-band: vía paquetes RTP en banda.
	- RFC2833: vía paquetes RTP RFC2833.
Hook Flash Relay setting	Especifica que evento se utiliza cuando se transmite eventos hook
	flash. Los posibles valores son:
	- SIPInfo: vía paquetes SIP INFO.
	- None: No trasnsmite eventos hook flash.
SIP Transport protocol	Especifica el protocolo de trasnsporte para los mensajes SIP salientes:
	- UDP
	- TCP
	- TLS

SRTP Configuration	Habilita SRTP (Secure Real-time Transport Protocol))
Enable SIP tag matching	Especifica si la etiqueta tiene que coincidir estrictamente para la confirmación de los diálogos SIP en todas las sesiones SIP.
Music Server	Nombre o dirección IP de un servidor de música
Music Server port	Puerto del servidor de música
Conference URI	URI de una conferencia.
Conference Option	Sólo es posible especificar la opción LOCAL

Diagnostics

Este apartado el resultado del test a cada interfaz de la red local. Para asegurarnos del estado actual de cada test, pulsar *"Rerun Diagnostics Tests"*. Si el resultado del test es *"FAIL"*, pulsa *"Help"* y sigue los procedimientos de *troubleshooting*.

📕 🛅 Fiber Home Gateway 🛛 🗙				Bearing and an and an and a state of the sta
	/192.168.1.1:8080/main.h	tml		
M movistar				
	Diagnostics The individual tests are listed below.	If a test	display	s a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.
Device Info	Test the connection to your local	netwo	rk	
Advanced Setup	Test your eth0 Connection:	FAIL	Heip	
Voice	Test your eth1 Connection:	PASS	Help	
Diagnostics	Test your eth2 Connection:	FAIL	Help	
Management	Test your eth3 Connection:	FAIL	Help	
	Test your eth4 Connection:	PASS	Help	
	Test your Wireless Connection:	PASS	Help	
				Rerun Diagnostic Tests

Management

Settings

Esta sección incluye las siguientes opciones: "Backup Settings", "Update Settings" y "Restore Default".

Backup

Para salvar la configuración actual a un fichero, haga clic en el botón "*Backup Settings*". Se le pedirá una localización en su PC donde guardar el fichero de seguridad. Este fichero puede ser recuperado posteriormente utilizando el botón "*Update Settings*" descrito a continuación.

Update

Esta opción recupera el fichero de configuración salvado anteriormente utilizando el botón "*Backup Settings*". Introduzca el nombre del fichero (incluyendo su localización) en el campo "*Settings File name*" o haga clic en el botón "*Browse Default Settings*" para buscar el fichero. Haga clic en el botón "*Update Settings*" para recuperar la configuración.

Restore Default

Haga Clic en el botón "*Restore Default Settings*" para restaurar los valores de fábrica o por defecto. Después de cliquear el botón "*Restore Default Settings*", se mostrará el siguiente mensaje:

DSL Router Restore

The DSL Router configuration has been restored to default settings and the router is rebooting. Close the DSL Router Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

Cierre el navegador y espere 2 minutos antes de reabrirlo. Puede ser necesario, reconfigurar la configuración IP de su PC para que coincide con la nueva configuración.

TR-069 Client

WAN Management Protocol (TR-069) permite a un Auto-Configuration Server (ACS) llevar a cabo la autoconfiguración, provisión, colección, y diagnósticos del dispositivo. Seleccione los valores deseados y haga clic en el botón "Apply/Save" para configurar las opciones del cliente TR-069.



Campo	Descripción
Inform	Activa/desactiva el cliente TR-069
Inform Interval	La duración del intervalo en segundos para la cual el TriWave debe atender la conexión con el ACS y llamar al método " <i>Inform</i> ".
ACS URL	URL para el CPE para conectarse al ACS utilizando <i>WAN Management Protocol</i> . Este parámetro debe tener formato URL valido para HTTP o HTTTPS. Una URL HTTPS indica que el ACS soporta SSL. El CPE usa un certificado para validarse en al URL del ACS donde se realiza una autenticación basada en certificado.
ACS User Name	Nombre de usuario utilizado para autenticar el TriWave cuando se realiza una conexión al ACS utilizando <i>WAN Management Protocol</i> . Este nombre de usuario es usado solo para autenticación HTTP por el TriWave.

ACS Password	Contraseña utilizada para autenticar el TriWave cuando se realiza una conexión al ACS
	utilizando WAN Management Protocol. Esta contraseña es usada solo para
	autenticación HTTP por el TriWave.
WAN Interface used by	Seleccionar "Any_WAN", "LAN", "Loopback" o una conexión configurada.
TR-069 client	
Display SOAP messages	Activa/desactiva Mensajes SOAP o consola serie. Esta opción es usada para
on serial console	troubleshooting avanzado del TriWave.
Solicitud de conexión	
Authentication	Marca la casilla para activarlo
User Name	Nombre de usuario usado para autenticar una solicitud de conexión realizada a un ACS
	por el TriWave.
Password	Contraseña usada para autenticar una solicitud de conexión realizada a un ACS por el
	TriWave.
URL	Universal Resource Locator.

El botón "*Get RPC Methods*" fuerza que el CPE establezca una conexión inmediata al ACS. Este debe ser usado para descubrir los métodos de configuración soportados por el ACS o por el CPE. Esta lista debe incluir ambos métodos estándar TR-069 (Estas definiciones en la especificación o en versiones posteriores) y métodos específicos del proveedor. El receptor de la respuesta debe ignorar cualquier método irreconocible.

Internet Time

/ m

Esta opción sincroniza automáticamente el tiempo y hora del router con un servidor de tiempo de internet. Para habilitar la sincronización horaria, marque la correspondiente casilla de verificación, seleccionando el servidor de tiempo preferido, seleccionar la correcta zona horaria y haga clic en el botón "*Save/Apply*".

n.	
n.	
n.	
n.	
1.	
ers	
-	
Inora.ngn.rima-tde.net	
m 🔻	
T	
T	
T	
Brussels, Copenhagen, Madrid, Paris 🔹 🔹	
	HS

<u>Nota</u>: Internet Time debe estar activado para usar el Parental Control Además, este menú no es mostrado en modo Bridge, ya que el TriWave no sería capaz de conectar con el servidor NTP.

Access Control

Passwords

Esta pantalla es usada para configurar la contraseña de las cuentas de usuarios utilizadas para acceder el dispositivo. El acceso al TriWave es controlado a través del siguiente árbol de usuarios:

1234: Tiene acceso sin restricciones para cambiar y visualizar la configuración.

Support: Usado para mantenimiento remoto y diagnóstico del router.

User: Tiene acceso limitado. Esta cuenta puede ver los parámetros de configuración y estadísticas, así como, actualizar el firmware del router.

Use los siguientes campos para cambiar los parámetros de la contraseña. Haga clic en el botón "*Save/Apply*" para continuar.



Nota: La contraseña o password debe tener máximo, 16 caracteres.

Update Software

Esta opción permite llevar a cabo una actualización de firmware desde un fichero almacenado de forma local.



- Paso 1: Obtener el fichero imagen de la versión de software a actualizar desde su ISP.
- Paso 2: Introduzca la ruta y nombre de fichero de la imagen de versión de software en el campo
 "Software File Name" o haga clic en el botón *Browse* para localizar el fichero imagen.
- **Paso 3:** Haga clic en el botón Update Software una vez para actualizar e instalar el fichero.

Nota: El proceso de actualización durará aproximadamente 2 minutos para completarse. El dispositivo se reiniciará y la ventana del navegador se refrescará a la pantalla por defecto si la instalación ha sido satisfactoria. Es recomendable que se compare la versión de software en la parte alta de la pantalla Device Info con la versión de firmware instalada, para confirmar la instalación satisfactoria.

Reboot

Para guardar la configuración actual y reiniciar el router haga clic en el botón "Save/Reboot".

Nota: Es necesario cerrar la ventana del navegador y esperar 2 minutos antes de reabrirla. Es necesaria también para resetear la configuración IP de su PC.

Información para el tratamiento de los equipos eléctricos y electrónicos al final de su vida útil (Aplicable en

la UE y en países europeos con sistemas de recogida selectiva de residuos)

Este símbolo en el equipo, embalaje o manual de instrucciones indica que este producto, al final de su vida útil, no puede tratarse como un residuo doméstico normal, sino que debe ser recogido de forma selectiva.



Al entregar este producto para su gestión ambiental está evitando las posibles consecuencias negativas para el medio ambiente y la salud derivadas de una eliminación inadecuada. Además, mediante el reciclaje de los materiales que componen este producto se obtiene un ahorro importante de energía y recursos.

Para la recogida selectiva del producto puede contactar con el Dpto. Comercial de TELNET Redes Inteligentes S.A. en el teléfono 976.14.18.00, con su distribuidor habitual o consultar la página web <u>www.telnet-ri.es</u>

En cumplimiento del RD 208/2005, TELNET Redes Inteligentes S.A. participa en el Sistema Integrado de Gestión (SIG) de la Fundación ECOTIC



TELNET Redes Inteligentes S.A. se encuentra inscrito en el Registro nacional de productores de aparatos eléctricos y electrónicos (REI-RAEE) del Ministerio de Industria, Turismo y Comercio con el número 1746



©2014 TELNET Redes Inteligentes S.A. Todos los derechos reservados

Toda la información contenida o revelada por el presente documento se considera confidencial y patentada por TELNET Redes Inteligentes SA. se reserva el derecho de utilizar este diseño en otros proyectos sin referencia al destinatario. Al aceptar este material, el beneficiario acuerda que este material y la información contenida en los mismos se gestionada con discreción y con confianza y no serán copiada o revelada en su totalidad o en parte, a cualquier tercero.