

## EDIMAX:

Así se ve la dirección del servidor al principio, se la cambiamos.

The screenshot shows the 'General Setup' tab selected in the top navigation bar. Under the 'Time Zone' section, the 'Set Time Zone' dropdown is set to '(GMT+01:00)Barcelona, Madrid'. Below it, the 'Time Server Address' field contains '192.43.244.18'. The 'Daylight Savings' section includes a checkbox for 'Enable Function' and dropdown menus for 'January' and '1'. A red 'Apply' button is at the bottom right. To the right, a 'Help' sidebar provides information about the time zone and password settings.

Le cambiamos la contraseña que tenía anteriormente para acceder al router por una nueva.

The screenshot shows the 'General Setup' tab selected. In the 'Password Settings' section, there are fields for 'Current Password', 'New Password', and 'Confirmed Password', each containing four dots. Below these is a red 'Apply' button. To the right, a 'Help' sidebar explains the password change function.

Para identificarla de manera más fácil, cambiamos el nombre de la red.

The screenshot shows the 'General Setup' tab selected. In the 'Wireless Settings' section, the 'Mode' dropdown is set to 'AP', 'Band' to '2.4 GHz (B+G+N)', and 'ESSID' to 'GALAM'. Other fields include 'Channel Number' (11) and 'Associated Clients' (>Show Active Clients<). A red 'Apply' button is at the bottom right. To the right, a 'Help' sidebar provides details on wireless basic settings, security, and MAC address filtering.

Para hacerla más segura, cambiamos el tipo de encriptación y le ponemos una contraseña para poder acceder de manera inalámbrica a la red.

The screenshot shows the 'General Setup' > 'Wireless' configuration page. Under 'Wireless Settings', the encryption is set to 'WPA pre-shared key'. The 'Security Settings' section contains fields for 'Pre-shared Key Format' (set to 'Passphrase') and 'Pre-shared Key' (set to 'GALAM2020'). The 'MAC Address Filtering' and 'WPS(Wi-Fi Protected Setup) Settings' sections are also visible. On the right, a 'Help' sidebar provides links to 'Wireless Basic Settings', 'Wireless Advanced Settings', 'Security Settings', 'MAC Address Filtering', and 'WPS(Wi-Fi Protected Setup) Settings'.

Mediante el filtrado MAC por lista blanca, ingresamos las MAC de los dispositivos que SÍ se van a conectar a la red, todos los demás dispositivos que intenten acceder, no podrán.

The screenshot shows the 'General Setup' > 'Wireless' configuration page with the 'MAC Address Filtering' tab selected. It displays a table of allowed MAC addresses, each with a 'Comment' field and checkboxes for 'Delete Selected' and 'Delete All'. The table includes entries for 'Móvil GEO', 'Móvil María', and 'Móvil Lore'. The 'WPS(Wi-Fi Protected Setup) Settings' section is also present. The right sidebar provides help for various wireless settings.

Metemos la MAC de los móviles de 3 de los 4 integrantes del grupo, estos 3 pueden conectarse a la red sin problemas.

This screenshot is identical to the one above, showing the 'General Setup' > 'Wireless' configuration page with the 'MAC Address Filtering' tab selected. The table lists the same three devices: 'Móvil GEO', 'Móvil María', and 'Móvil Lore'. The 'WPS(Wi-Fi Protected Setup) Settings' section is also present. The right sidebar provides help for various wireless settings.

Por ejemplo, aquí podemos ver el Móvil de Georgi y cómo sí puede acceder a la red y tiene conexión de manera funcional.

The image shows a side-by-side comparison of two mobile device screens. The left screen displays the Wi-Fi settings of a Samsung smartphone, showing a list of networks under 'CONECTADO' (Connected) and 'REDES DISPONIBLES' (Available Networks). The right screen shows a Google search results page for the query 'conexion aceptada' (connection accepted).

**Left Screen (Wi-Fi Settings):**

- 11:04 | Battery level: 82%
- Wi-Fi icon: On
- Section: CONECTADO
  - GALAM (Toca para compartir la contraseña)
  - Alumnos2016 (Guardado)
  - Andared (Guardada, conexión automática desactivada)
  - TeleAlcala\_Fibr...Optica\_oqcwot (Guardado)
- Section: REDES DISPONIBLES
  - MDJ (Actualizar)

**Right Screen (Google Search Results):**

- 11:06 | Battery level: 81%
- Google logo
- Search bar: conexión aceptada
- Results:
  - Conexión no aceptada por in lok - AYR (https://ayr.es/blog/soprotecnico): Empezó por no conectarse con un móvil y ahora son tres con los que no acepta conexión siempre funcionaron bien pero ahora no entiendo el por qué ...
  - Solucionado: Bluetooth no funciona - Samsung Community (https://eu.community.samsung.com/...): 1 SOLUCIÓN ACEPTADA. Soluciones aceptadas ... Hay dispositivos Bluetooth que solo permite una conexión a la vez y rechazan otras. Es decir, si tu ...
  - conectar | Definición | Diccionario de la lengua española | RAE - ASALE (https://dle.rae.es/conectar): 1. tr. Unir o poner en comunicación dos cosas o dos personas, o una con otra. Me conectaron con un especialista. U. t. c. intr. No llegaron a conectar ...
- Navigation icons: Back, Home, Stop
- Bottom menu: Discover, Notificaciones, Buscar, Colecciones, Más

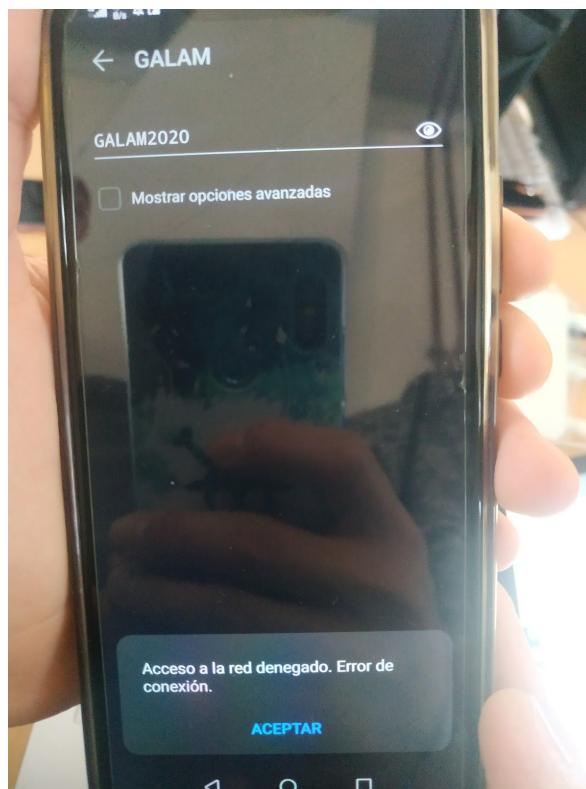
Aquí unas capturas del Móvil de Alejandro Lorenzo y también puede acceder.

The left screenshot shows the Wi-Fi settings on a mobile device. The 'Wi-Fi' switch is turned on, and the 'REDES DISPONIBLES' section lists three networks: 'GALAM' (Connected, good signal), 'Alumnos2016' (Saved, encrypted, normal signal), and 'PRUEBAS\_EECC' (Encrypted). The right screenshot shows a Google search result for 'ies fuente grande'. The top result is 'IES Fuente Grande' (Secondary school in Alcalá del Valle, 75m, Open), with options to 'RESUMEN', 'RESEÑAS', or 'FOTOS'. Below the summary is the address 'Calle Blas Infante, SN, 11693 Alcalá del Valle, Cádiz' and a map pin.

Y lo mismo con el Móvil de María, conseguimos conectarnos sin problemas.

The left screenshot shows the Wi-Fi settings on a mobile device. The 'Wi-Fi' switch is turned on, and the 'CONECTADO' section shows 'GALAM' (Connected) with a note to share the password and 'Alumnos2016' (Saved). The right screenshot shows a Google search result for 'seijuro mikoshiba'. The top result is 'Seijuro Mikoshiba' (Character from fiction), with options to '+ Seguir', 'RESUMEN', 'INTERPRETADO POR', or 'PROGRAMA DE TV'. Below the summary are three profile pictures of the character. A callout box at the bottom provides additional information: 'Interpretado por: Kenjirō Tsuda' and 'programa de TV: Free!'

Pero desde el móvil de Antonio, como no está incluido en la lista blanca, no le deja acceder a la red. (no deja hacer captura de pantalla así que le sacamos una foto).



Para que sea más segura la red, desactivamos el WPS

Home   Quick Setup   **General Setup**   iQoS   Status   Tools

System | WAN | LAN | **Wireless** | Advanced Settings | NAT | Firewall | Parental Control |

**Wireless Settings**

**Security Settings**

**MAC Address Filtering**

**WPS(Wi-Fi Protected Setup) Settings**

Enable WPS

Wi-Fi Protected Setup Information :

WPS Status: : Configured

Self PinCode: : 73870203

SSID: : GALAM

Authentication Mode: : WPA pre-shared key

Authentication Key: : GALAM2020

Device Configure

Config Mode

Configure via Push Button :

Configure via Client PinCode :

**Help**

**Wireless Basic Settings**  
This page allows you to define ESSID and Channel for the wireless connection. These parameters are used by ....[more](#)

**Wireless Advanced Settings**  
These settings are only suitable for experienced users who have required knowledge about wireless LAN. This ....[more](#)

**Security Settings**  
This page allows you to setup wireless security. You can protect your wireless network by using WEP / WPA....[more](#)

**MAC Address Filtering**  
To improve security, this access point features MAC address filtering function that only allows listed MA....[more](#)

**WPS(Wi-Fi Protected Setup) Settings**  
You can change WPS (Wi-Fi Protected Setup) settings in this page. WPS will help your wireless client to con....[more](#)

Mediante el control parental, añadimos la dirección MAC del dispositivo que queramos que no se conecte a la red a ciertas horas de determinados días.

**Parental Control Rule**

MAC: 9CD21E8B174A	<> Select
Weekdays: <input checked="" type="checkbox"/> Sun <input type="checkbox"/> Mon <input checked="" type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input checked="" type="checkbox"/> Sat	
Time Start: Hour 16 Minute 00	Time Stop: Hour 19 Minute 00

**Buttons:** Add, Reset, Delete, Delete All, Select, APPLY, CANCEL

Vemos cómo ha sido añadida, en este caso la MAC de María, por lo cual no le dejará conectarse a la red a dicha hora

**Parental Control Rule**

MAC: 9CD21E8B174A	<> Select
Weekdays: <input type="checkbox"/> Sun <input checked="" type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat	
Time Start: Hour 14 Minute 00	Time Stop: Hour 15 Minute 00

**Buttons:** Add, Reset, Delete, Delete All, Select, APPLY, CANCEL

Vemos aquí cómo intenta conectarse a la Red, pero directamente no le carga ninguna página debido al control parental que le hemos puesto anteriormente.



### No se puede acceder a este sitio web

[www.youtube.com](http://www.youtube.com) ha tardado demasiado tiempo en responder.

Prueba a:

- Comprobar la conexión
- Comprobar el proxy y el cortafuegos
- Ejecutar Diagnósticos de red de Windows

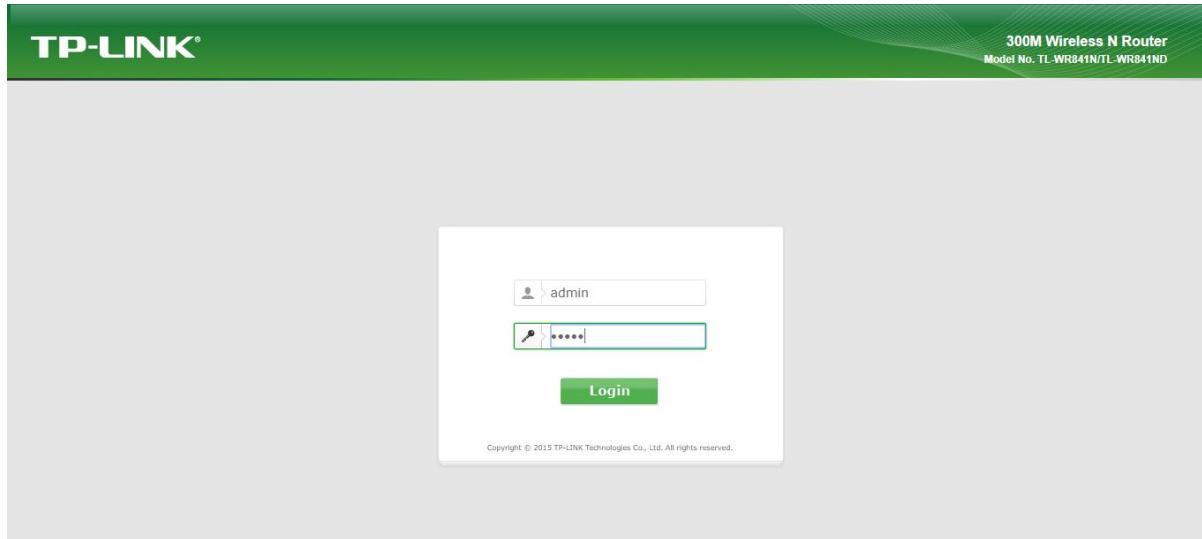
ERR\_CONNECTION\_TIMED\_OUT

[Volver a cargar](#)

[Detalles](#)

## TP-LINK:

Para configurar el router debemos irnos al buscador y escribir la IP del router (suele ser XX.XX.XX.1), una vez insertada, iniciaremos sesión con el usuario y contraseña “admin”.



Cuando logremos iniciar con el usuario, nos dirigiremos a “Quick Setup” y empezaremos a editar los datos. En este caso hemos cambiado el nombre de la red a GALAM y la contraseña GALAM2020.

The Internet settings have been completed, now please configure the wireless settings.

Wireless Radio:

Wireless Network Name:  (Also called the SSID)

Region:

Warning: Ensure you select a correct country to conform local law. Incorrect settings may cause interference.

Wireless Security:

Disable Security

WPA-PSK/WPA2-PSK

Wireless Password:   
(You can enter ASCII characters between 8 and 63 or Hexadecimal characters between 8 and 64.)

No Change  
(use the current security settings.)

More Advanced Wireless Settings

**Wireless Help**

Wireless Radio - Enable or disable the wireless radio.

Wireless Network Name - Enter a string of up to 32 characters. The same Name (SSID) must be assigned to all wireless devices in your network. The default SSID is set to be **TP-LINK\_xxxx** (xxxx indicates the last unique four characters of each Router's MAC address), which can ensure your wireless network security. But it is recommended strongly that you change your networks name (SSID) to a different value. This value is case-sensitive. For example, **MYSID** is NOT the same as **MySID**.

Region - Select your region from the pull-down list. This field specifies the region where the wireless function of the Router can be used. It may be illegal to use the wireless function of the Router in a region other than one of those specified in the field. If your country or region is not listed, please contact your local government agency for assistance.

You can select one of the following security options:

Disable Security - The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the Router without encryption. It is recommended strongly that you choose one of following options to enable security.

WPA-PSK/WPA2-PSK - Select WPA based on pre-shared passphrase.

- PSK Password - You can enter ASCII or Hexadecimal characters.
- For ASCII, the length should be between 8 and 63 characters.
- For Hexadecimal, the length should be between 8 and 64 characters.

Please note that the key is case sensitive.

Si nos vamos al siguiente apartado de la lista que nos aparece a la izquierda, podremos cambiar el Pin para WPS (yo lo dejé predeterminado).

**TP-LINK®**

300M Wireless N Router  
Model No. TL-WR841N / TL-WR841ND

- Status
- Quick Setup
- WPS**
- Network
- Wireless
- Guest Network
- DHCP
- Forwarding
- Security
- Parental Control
- Access Control
- Advanced Routing
- Bandwidth Control
- IP & MAC Binding
- Dynamic DNS
- IPv6 Support
- System Tools
- Logout

### WPS (Wi-Fi Protected Setup)

SSID:	GALAM
WPS Status:	Enabled <input type="button" value="Disable WPS"/>
Current PIN:	74894673 <input type="button" value="Restore PIN"/> <input type="button" value="Gen New PIN"/> <input type="checkbox"/> Disable PIN of this device
Add a new device:	<input type="button" value="Add Device"/>

**Wi-Fi Protected Setup Help**

WPS function will help you add a new device to the network quickly. If the new device supports Wi-Fi Protected Setup and is equipped with a configuration button, you can add it to the network by pressing its own configuration button. You can press the button on this device within two minutes. The status LED on this device will light green for five minutes if the new device has been successfully added to the network. If the new device supports Wi-Fi Protected Setup and the connection way using PIN, you can add it to the network by entering this device's PIN.

- **WPS Status** - Enable or disable the WPS function here.
- **Current PIN** - The current value of this device's PIN, displayed here. The default value can be found in the label of User Guide.
- **Restore PIN** - Restore the PIN of this device to its default.
- **Gen New PIN** - Click this button, and then you can get a new random value for this device's PIN. You can ensure the network security by generating a new PIN.
- **Disable PIN of this device** - WPS external registrar of entering this device's PIN can be disabled or enabled manually. If this device receives multiple failed attempts to authenticate an external registrar, this function will be disabled automatically.
- **Add Device** - You can add the new device to the existing network manually by clicking this button.

Note: The WPS function cannot be configured if the Wireless Function of this device is disabled. Please make sure the Wireless Function is enabled before configuring the WPS.

Si seguimos bajando, nos encontraremos con la opción de cambiar el tipo de conexión a Dinámico, Estático, etc.

**TP-LINK®**

300M Wireless N Router  
Model No. TL-WR841N / TL-WR841ND

- Status
- Quick Setup
- WPS**
- Network**
- WAN
- MAC Clone
- LAN
- Wireless
- Guest Network
- DHCP
- Forwarding
- Security
- Parental Control
- Access Control
- Advanced Routing
- Bandwidth Control
- IP & MAC Binding
- Dynamic DNS
- IPv6 Support
- System Tools
- Logout

**WAN Connection Type:**

IP Address:	192.168.18.43
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.18.1
	<input type="button" value="Renew"/> <input type="button" value="Release"/>
MTU Size (in bytes):	1500 <small>(The default is 1500, do not change unless necessary.)</small>
<input type="checkbox"/> Use These DNS Servers	
Primary DNS:	192.168.18.1
Secondary DNS:	0.0.0.0 <small>(Optional)</small>
Host Name:	TL-WR841N
<input type="checkbox"/> Get IP with Unicast DHCP (It is usually not required.)	

**WAN Help**

**WAN Connection Type:**

If your ISP is running a DHCP server, select the **Dynamic IP** option.

If your ISP provides a static or fixed IP Address, Subnet Mask, Gateway and DNS setting, select the **Static IP** option.

If your ISP provides a PPPoE connection, select **PPPoE/Russia PPPoE** option.

If your ISP provides BigPond Cable (or Heart Beat Signal) connection, please select **BigPond Cable** option.

If your ISP provides L2TP connection, please select **L2TP/Russia L2TP** option.

If your ISP provides PPTP connection, please select **PPTP/Russia PPTP** option.

If you don't know how to choose the appropriate connection type, click the **Detect** button to allow the Router to automatically search your Internet connection for servers and protocols. The connection type will be reported when an active Internet service is successfully detected by the Router. This report is for your reference only. To make sure the connection type your ISP provides, please refer to the ISP. The various types of Internet connections that the Router can detect are as follows:

- **PPPoE/Russia PPPoE** - Connections which use PPPoE that requires a user name and password.
- **Dynamic IP** - Connections which use dynamic IP address assignment.
- **Static IP** - Connections which use static IP address assignment.

En el segundo apartado dentro de Network, podemos cambiar la MAC.

**TP-LINK®**

300M Wireless N Router  
Model No. TL-WR841N / TL-WR841ND

- Status
- Quick Setup
- WPS**
- Network**
- WAN
- MAC Clone
- LAN
- Wireless
- Guest Network
- DHCP
- Forwarding
- Security
- Parental Control
- Access Control
- Advanced Routing
- Bandwidth Control
- IP & MAC Binding
- Dynamic DNS
- IPv6 Support
- System Tools
- Logout

### MAC Clone

WAN MAC Address:	84-16-F9-29-67-99	<input type="button" value="Restore Factory MAC"/>
Your PC's MAC Address:	8C-16-45-8C-3C-9B	<input type="button" value="Clone MAC Address"/>
<input type="button" value="Save"/>		

**MAC Clone Help**

Some ISPs require that you register the MAC Address of your adapter. Usually, you do not need to change anything here.

**WAN MAC Address** - This field displays the current MAC address of the WAN port. If your ISP requires that you register the MAC address, please enter the correct MAC address into this field. The format for the MAC Address is XX-XX-XX-XX-XX-X (X is any hexadecimal digit).

**Your PC's MAC Address** - This field displays the MAC address of the PC that is managing the Router. If the MAC address of your adapter is registered, you can click the **Clone MAC Address** button, and then it will be filled into the **WAN MAC Address** field.

Click **Restore Factory MAC** to restore the MAC address of WAN port to the factory default value.

Click the **Save** button to save your settings.

**Note:**

1. Only the PC(s) in your LAN can use the **MAC Address Clone** feature.
2. If you change **WAN MAC Address** when the WAN connection type is **PPPoE**, it will not take effect until the connection is re-established.

En este último apartado modificaremos la IP y pondremos la que queramos.

The screenshot shows the 'LAN' configuration page. On the left, a navigation menu lists various network-related options like Status, Quick Setup, WPS, Network, WAN, MAC Clone, LAN, Wireless, Guest Network, DHCP, Forwarding, Security, Parental Control, Access Control, Advanced Routing, Bandwidth Control, IP & MAC Binding, Dynamic DNS, IPv6 Support, System Tools, and Logout. The 'Network' option is currently selected. The main panel displays fields for MAC Address (84-16-F9-29-67-98), IP Address (192.168.15.1), Subnet Mask (255.255.255.0), and IGMP Proxy (Enable). A note at the bottom states: 'Note: IGMP(Internet Group Management Protocol) works for IPTV multicast stream. The device supports both IGMP proxy with enabled/disabled option and IGMP snooping.' Below these fields is a 'Save' button. To the right, a 'LAN Help' section provides instructions for changing the LAN IP address, noting that the new address must be in the same subnet as the previous one. It also mentions that the Virtual Server and DMZ Host will be re-configured automatically if the new address is different. A note at the bottom of this section says: 'Click the Save button to save your settings.'

En el apartado “Wireless”, cambiaremos el nombre de la red y el país.

The screenshot shows the 'Wireless Settings' configuration page. The left navigation menu includes options like Status, Quick Setup, WPS, Network, Wireless, Wireless Settings, Wireless Security, Wireless MAC Filtering, Wireless Advanced, Wireless Statistics, Guest Network, DHCP, Forwarding, Security, Parental Control, Access Control, Advanced Routing, Bandwidth Control, IP & MAC Binding, Dynamic DNS, and IPv6 Support. The 'Wireless' option is selected. The main panel has fields for Wireless Network Name (GALAM), Region (Spain), Mode (11bgn mixed), Channel Width (Auto), and Channel (11). Underneath these are checkboxes for 'Enable Wireless Router Radio', 'Enable SSID Broadcast', and 'Enable WDS Bridging'. A 'Save' button is located at the bottom. To the right, a 'Wireless Settings Help' section provides notes about the operating distance, region selection, and channel guidelines. It also includes detailed descriptions for each field and their effects on performance and security.

Es recomendable cambiar la contraseña ya que sería muy vulnerable.

The screenshot shows the 'Wireless Security' configuration page. The left navigation menu includes the same set of options as the previous screen. The 'Wireless' option is selected. The main panel features two tabs: 'Disable Security' (selected) and 'WPA/WPA2 - Personal (Recommended)'. The 'WPA/WPA2 - Personal' tab contains fields for Version (Automatic), Encryption (AES), Wireless Password (GALAM2020), and Group Key Update Period (0 seconds). Below this is another tab for 'WPA/WPA2 - Enterprise', which includes fields for Version (Automatic), Encryption (Automatic), Radius Server IP, Radius Port (1812), Radius Password, and Group Key Update Period (0 seconds). To the right, a 'Wireless Security Help' section provides information on security options like Disable Security, WPA/WPA2 - Personal, and WPA/WPA2 - Enterprise. It also details the settings for each security type, including password length requirements and update intervals.

También para mejorar la seguridad podemos hacer un filtro de MAC, de ese modo solo las MAC que estén apuntadas podrán conectarse a la red.

The screenshot shows the 'Wireless MAC Filtering' section of the router's web interface. On the left, a sidebar lists various configuration options like Status, Quick Setup, WPS, Network, and Wireless. The 'Wireless MAC Filtering' option is selected. The main content area has a green header 'Wireless MAC Filtering'. Below it, there's a status bar with 'Wireless MAC Filtering: Disabled' and an 'Enable' button. A 'Filtering Rules' section follows, containing two radio buttons: 'Deny' (selected) and 'Allow'. A table lists a single rule: ID 1, MAC Address 24-D4-33-2F-D1-7E, Status Enabled, Description Móvil Antonio. Buttons for 'Add New...', 'Enable All', 'Disable All', and 'Delete All' are available. At the bottom are 'Previous' and 'Next' navigation buttons. To the right is a 'Wireless MAC Filtering Help' section with instructions and a status table.

Este es un ejemplo en el cual añado una MAC, en este caso mi móvil.

This screenshot shows the 'Add or Modify Wireless MAC Address Filtering entry' page. The sidebar and main layout are identical to the previous screenshot, but the central table now contains a single row with the MAC address 24-D4-33-2F-D1-7E, a status of 'Enabled', and a description 'Móvil Antonio'. Below the table are 'Save' and 'Back' buttons. To the right is a 'Wireless MAC Filtering Help' section with instructions and a status table.

Quedaría así:

The screenshot shows the 'Wireless MAC Filtering' page after adding the MAC entry. The table now includes the new rule: ID 1, MAC Address 24-D4-33-2F-D1-7E, Status Enabled, and Description Móvil Antonio. The 'Modify' and 'Delete' buttons are visible next to the row. The rest of the interface and help section remain the same.

Ahora podemos editar el ancho de banda, no lo modifco. Si nos vamos a la parte inferior, encontraremos la opción para cambiar el nombre a Network.

The screenshot shows the 'Guest Network Wireless Settings' page. On the left sidebar, 'Guest Network' is selected. The main area has two sections: 'Access And Bandwidth Control' and 'Wireless'. In 'Access And Bandwidth Control', 'Allow Guest To Access My Local Network' is checked. 'Enable Guest Network Bandwidth Control' is checked, and bandwidth values are set to 256 Kbps (Range: 1~100000) for Egress and 1024 Kbps (Range: 1~100000) for Ingress. In the 'Wireless' section, 'Guest Network' is checked, and the network name is set to 'GALAM2020'. Security is set to WPA/WPA2-Personal, Version to WPA2-PSK, Encryption to AES, and PSK Password to '74894673'. A note indicates that ASCII characters between 8 and 63 or Hexadecimal characters can be used. The Group Key Update Period is set to 0 seconds. The 'Access Time' dropdown is set to 'Schedule' with the message 'can not be connected.' Below the schedule dropdown are checkboxes for 'Everyday' and 'Select Days', followed by days of the week checkboxes. Start and End Time fields are present. A 'Save' button is at the bottom.

También nos permite habilitar un rango de tiempo operativo.

This screenshot shows the same 'Guest Network Wireless Settings' page as above, but the 'Access Time' dropdown is expanded to show 'Schedule' and 'can not be connected.' Below the dropdown are checkboxes for 'Everyday' and 'Select Days', followed by days of the week checkboxes. There are also checkboxes for 'All day-24 Hours', 'Start Time' (HHMM), and 'End Time' (HHMM). A 'Save' button is at the bottom.

Si queremos establecer DHCP con la siguiente modificación nos lo permitirá. Esto es opcional. Añadimos el rango de IP, la puerta de enlace y el nombre del dominio.

The screenshot shows the 'DHCP Settings' page. On the left sidebar, 'DHCP' is selected. The main area has fields for 'DHCP Server' (set to 'Enable'), 'Start IP Address' (192.168.15.100), 'End IP Address' (192.168.15.199), 'Address Lease Time' (120 minutes), 'Default Gateway' (192.168.15.1), 'Default Domain' (Galam2020), 'Primary DNS' (0.0.0.0), and 'Secondary DNS' (0.0.0.0). A 'Save' button is at the bottom. To the right, there is a 'DHCP Settings Help' section with detailed explanations for each field and a note about using the DHCP server function.

De esta forma se añaden los dispositivos al DHCP. Pulsamos sobre “Add New”.

Insertamos la MAC y la IP del dispositivo.

Debería quedar así:

En este punto donde se puede modificar la seguridad, recomiendo no editarlo.

**TP-LINK®**

**300M Wireless N Router**  
Model No. TL-WR841N / TL-WR841ND

**Basic Security**

**Firewall**

SPI Firewall:  Enable  Disable

**VPN**

PPTP Passthrough:  Enable  Disable  
L2TP Passthrough:  Enable  Disable  
IPSec Passthrough:  Enable  Disable

**ALG**

FTP ALG:  Enable  Disable  
TFTP ALG:  Enable  Disable  
H323 ALG:  Enable  Disable  
RTSP ALG:  Enable  Disable  
SIP ALG:  Enable  Disable

**Save**

**Basic Security Help**

You can configure the Basic Security Settings on this page.

**Firewall** - Here you can enable or disable the Router's firewall.

- SPI Firewall - Stateful Packet Inspection (SPI) helps to prevent cyber attacks by tracking more state per session. It validates that the traffic passing through the session conforms to the protocol. SPI Firewall is enabled by factory default. If you want all the computers on the LAN exposed to the outside world, you can disable it.

**VPN** - VPN Passthrough must be enabled if you want to allow VPN tunnels using VPN protocols to pass through the Router.

- PPTP Passthrough - PPTP Passthrough Point-to-Point Tunneling Protocol (PPTP) is a Point-to-Point Protocol (PPP) to be tunneled through an IP network. To allow PPTP tunnels to pass through the Router, click Enable.
- L2TP Passthrough - Layer Two Tunneling Protocol (L2TP) is the method used to enable Point-to-Point sessions via the Internet at the Layer Two level. To allow L2TP tunnels to pass through the Router, click Enable.
- IPSec Passthrough - Internet Protocol security (IPSec) is a suite of protocols for encrypting private, secure communications over public, shared, Protocol (IP) networks, through the use of cryptographic security services. To allow IPSec tunnels to pass through the Router, click Enable.

**ALG** - It is recommended to enable Application Layer Gateway (ALG) because ALG allows customized Network Address Translation (NAT) traversal filters to be plugged into the gateway to support address and port translation for certain application layer "control/data" protocols such as FTP, TFTP, H323 etc.

**TP-LINK®**

**300M Wireless N Router**  
Model No. TL-WR841N / TL-WR841ND

**Advanced Security**

**Packets Statistics Interval (5 ~ 60):** 10 Seconds

**DoS Protection:**  Disable  Enable

Enable ICMP-FLOOD Attack Filtering  
**ICMP-FLOOD Packets Threshold (5 ~ 3600):** 50 Packets/Secs

Enable UDP-FLOOD Filtering  
**UDP-FLOOD Packets Threshold (5 ~ 3600):** 500 Packets/Secs

Enable TCP-SYN-FLOOD Attack Filtering  
**TCP-SYN-FLOOD Packets Threshold (5 ~ 3600):** 50 Packets/Secs

Ignore Ping Packet from WAN Port to Router  
 Forbid Ping Packet from LAN Port to Router

**Save** **Blocked DoS Host List**

**Advanced Security Help**

Using the Advanced Settings page, you can protect the Router from being attacked by TCP-SYN Flood, UDP Flood and ICMP-Flood.

Note: FLOOD Filtering will take effect only when the Traffic Statistics in System Tools is enabled.

- Packets Statistics Interval (5~60) - The default value is 10. Select a value between 5 and 60 seconds in the pull-down list. The Packets Statistic interval value indicates the time section of the packets statistic. The result of the statistic used for analysis by SYN Flood, UDP Flood and ICMP-Flood.
- DoS Protection - Enable or Disable the DoS protection function. Only when it is enabled, will the flood filters be enabled.
- Enable ICMP-FLOOD Attack Filtering - Enable or Disable the ICMP-FLOOD Attack Filtering.
- ICMP-FLOOD Packets Threshold (5~3600) - The default value is 50. Enter a value between 5 ~ 3600. When the current ICMP-FLOOD Packets number is beyond the set value, the Router will startup the blocking function immediately.
- Enable UDP-FLOOD Filtering - Enable or Disable the UDP-FLOOD Filtering.
- UDP-FLOOD Packets Threshold (5~3600) - The default value is 500. Enter a value between 5 ~ 3600. When the current UDP-FLOOD Packets number is beyond the set value, the Router will startup the blocking function immediately.
- Enable TCP-SYN-FLOOD Attack Filtering - Enable or Disable the TCP-SYN-FLOOD Attack Filtering.
- TCP-SYN-FLOOD Packets Threshold (5~3600) - The default value is 50. Enter a value between 5 ~ 3600. When the current TCP-SYN-FLOOD Packets numbers is beyond the set value, the Router will startup the blocking function immediately.
- Ignore Dns. Block from WAN Port to Router - Enable or

Este apartado nos ayuda a controlar a los más pequeños para que no se metan en páginas indebidas. Se añaden nuevos dispositivos pulsando sobre “Add New”.

**TP-LINK®**

**300M Wireless N Router**  
Model No. TL-WR841N / TL-WR841ND

**Parental Control Settings**

Non-Parental PCs not listed will not be able to access the Internet.

**Parental Control:**  Disable  Enable

**MAC Address of Parental PC:**   
**MAC Address of Your PC:** 8C-1E-45-8C-9B **Copy To Above**

**Save**

ID	MAC address	Website Description	Schedule	Status	Modify
Add New...	Enable All	Disable All	Delete All		

**Parental Control Settings Help**

The Router, providing convenient Parental Control function to control the internet activities of the child, can limit the child to access certain websites and restrict the time of surfing. On this page, you can create the rule.

- Parental Control - Check Enable if you want this function to take effect, otherwise check Disable.
- MAC Address of Parental PC - In this field, enter the MAC address of the controlling PC, or you can make use of the Copy To Above button below.
- MAC Address of Your PC - This field displays the MAC address of the PC that is managing this Router. If the MAC Address of your adapter is registered, you can click the Copy To Above button to fill this address to the MAC Address of Parental PC above.
- Website Description - Description of the allowed website for the PC controlled.
- Schedule - The time period allowed for the PC controlled to access the Internet. For detailed information, please go to Access Control > Schedule.
- Enable - Check this option to enable a specific entry.
- Modify - Here you can edit or delete an existing entry.

For example: If you desire that the child PC with MAC address 00-11-22-33-44-AA can access www.google.com on Saturday only while the parent PC with MAC address 00-11-22-33-44-BB is without any restriction, you should follow the settings below:

1. Click Parental Control menu on the left to enter the Parental Control Settings page. Check Enable and enter the MAC address 00-11-22-33-44-BB in the MAC Address of Parental PC field.

En esta lista añadimos las páginas que no queremos que se metan. Debe introducir la MAC del dispositivo.

Quedaría así:

Del apartado “Control de acceso” no he modificado nada. Aunque si lo editamos de una forma correcta, puede ser muy seguro ya que nos permite el control de la red sobre los otros dispositivos conectados a esta.

Podemos añadir rutas, las cuales hacen la conexión un poco más rápida.

**Static Routing Help**

A static route is a pre-determined path that network information must follow to reach a specific host or network. Use the Static Routing page to add or delete a route.

To add static routing entries:

- Click the Add New... button.
- Enter the following data:
  - Destination Network** - The Destination IP Address is the address of the network or host that you want to assign to a static route.
  - Subnet Mask** - The Subnet Mask determines which portion of an IP address is the network portion, and which portion is the host portion.
  - Default Gateway** - This is the IP address of the default gateway device that allows for the contact between the Router and the network or host.
- Select the Enabled in the Status pull-down list.
- Click the Save button to save the changes.

To modify or delete an existing entry:

- Find the desired entry in the table.
- Click Modify or Delete as desired on the Modify column.

Click the Enable All button to enable all entries.

Click the Disable All button to disable all entries.

Click the Delete All button to delete all entries.

Añadiremos la IP, la puerta de enlace y la máscara de subred.

**Static Routing Help**

A static route is a pre-determined path that network information must follow to reach a specific host or network. Use the Static Routing page to add or delete a route.

To add static routing entries:

- Click the Add New... button.
- Enter the following data:
  - Destination Network** - The Destination IP Address is the address of the network or host that you want to assign to a static route.
  - Subnet Mask** - The Subnet Mask determines which portion of an IP address is the network portion, and which portion is the host portion.
  - Default Gateway** - This is the IP address of the default gateway device that allows for the contact between the Router and the network or host.
- Select the Enabled in the Status pull-down list.
- Click the Save button to save the changes.

To modify or delete an existing entry:

- Find the desired entry in the table.
- Click Modify or Delete as desired on the Modify column.

Click the Enable All button to enable all entries.

Click the Disable All button to disable all entries.

Click the Delete All button to delete all entries.

Quedaría algo similar a esto:

**System Routing Table Help**

System routing table views all of the valid route entries in use. The Destination IP address, Subnet Mask, Gateway, and Interface will be displayed for each entry. Click the Refresh button to refresh the data displayed.

- Destination Network** - The Destination Network is the address of the network or host to which the static route is assigned.
- Subnet Mask** - The Subnet Mask determines which portion of an IP address is the network portion, and which portion is the host portion.
- Gateway** - This is the IP address of the gateway device that allows for contact between the Router and the network or host.
- Interface** - This interface tells you whether the Destination IP Address is on the LAN & WLAN (internal wired and wireless networks), the WAN (Internet).

Ahora definiremos la banda ancha que queremos.

**TP-LINK®**

300M Wireless N Router  
Model No. TL-WR841N / TL-WR841ND

- [Status](#)
- [Quick Setup](#)
- [WPS](#)
- [Network](#)
- [Wireless](#)
- [Guest Network](#)
- [DHCP](#)
- [Forwarding](#)
- [Security](#)
- [Parental Control](#)
- [Access Control](#)
- [Advanced Routing](#)
- Bandwidth Control**
- [Control Settings](#)
- [Rule List](#)
- [IP & MAC Binding](#)
- [Dynamic DNS](#)
- [IPv6 Support](#)
- [System Tools](#)
- [Logout](#)

### Bandwidth Control Settings

Enable Bandwidth Control:

Line Type:  ADSL  Other

Egress Bandwidth: 1024 Kbps

Ingress Bandwidth: 2048 Kbps

**Bandwidth Control Settings Help**

In this page you can disable or enable the Bandwidth Control feature. The Bandwidth Control Rules will work properly only when the Bandwidth Control feature is enabled.

- **Enable Bandwidth Control** - If enabled, the Bandwidth Control rules will take effect.
- **Line Type** - Please choose the line type you are using to make the bandwidth control module work properly.
- **Egress Bandwidth** - The upload speed through the WAN port.
- **Ingress Bandwidth** - The download speed through the WAN port.

Tendremos que cambiar la zona horaria y la hora ya que predeterminadamente está E.E.U.U.

**TP-LINK®**

300M Wireless N Router  
Model No. TL-WR841N / TL-WR841ND

- [Status](#)
- [Quick Setup](#)
- [WPS](#)
- [Network](#)
- [Wireless](#)
- [Guest Network](#)
- [DHCP](#)
- [Forwarding](#)
- [Security](#)
- [Parental Control](#)
- [Access Control](#)
- [Advanced Routing](#)
- [Bandwidth Control](#)
- [IP & MAC Binding](#)
- [Dynamic DNS](#)
- [IPv6 Support](#)
- System Tools**
- [Time Settings](#)
- [Diagnostic](#)
- [Firmware Upgrade](#)
- [Factory Defaults](#)

### Time Settings

Time zone: (GMT+01:00) Berlin, Stockholm, Rome, Bern, Brussels

Date: 3 12 2020 (MM/DD/YY)

Time: 16 51 00 (HH/MM/SS)

NTP Server 1: 0.0.0 (Optional)

NTP Server 2: 0.0.0 (Optional)

Enable DaylightSaving

Start: 2020 Mar Last Sun 1am

End: 2020 Oct Last Sun 1am

Daylight Saving Status:

Note: Click the "GET GMT" to update the time from the internet with the pre-defined servers or entering the customized server (IP Address or Domain Name) in the above frames.

**Time Settings Help**

This page allows you to set the time manually or to configure automatic time synchronization. The Router can automatically update the time from an NTP server via the Internet.

**Time Zone** - Select your local time zone from this pull-down list.

**To set time manually:**

1. Select your local time zone.
2. Enter the Date in Month/Day/Year format.
3. Enter the Time in Hour/Minute/Second format.
4. Click Save.

**For automatic time synchronization:**

1. Enter the address or domain of the NTP Server 1 or NTP Server 2.
2. Click the Get GMT button to get GMT from the Internet.

**To set up daylight saving:**

1. Select the Enable Daylight Saving checkbox to enable daylight saving function.
2. Enter the Start and End date and time of daylight saving range.
3. Click Save.

**Note:**

1. This setting will be used for some time-based functions such as firewall function. These time dependant functions will not work if time is not set. Therefore, it is important to specify time settings as soon as you successfully login to the Router.

También cambiaremos el usuario y contraseña al que queramos.

**TP-LINK®**

300M Wireless N Router  
Model No. TL-WR841N / TL-WR841ND

- [DHCP](#)
- [Forwarding](#)
- [Security](#)
- [Parental Control](#)
- [Access Control](#)
- [Advanced Routing](#)
- [Bandwidth Control](#)
- [IP & MAC Binding](#)
- [Dynamic DNS](#)
- [IPv6 Support](#)
- System Tools**
- [Time Settings](#)
- [Diagnostic](#)
- [Firmware Upgrade](#)
- [Factory Defaults](#)
- [Backup & Restore](#)
- [Reboot](#)
- [Password](#)
- [System Log](#)
- [Statistics](#)
- [Logout](#)

### Password

Username and password can contain between 1 - 15 characters and may not include spaces.

Old User Name:	admin
Old Password:	*****
New User Name:	GALAM
New Password:	*****
Confirm New Password:	*****

**Password Help**

It is strongly recommended that you change the factory default user name and password of this device. All users who try to access this device's web-based utility will be prompted for this device's user name and password.

**Note:** The new user name and password must not exceed 15 characters in length and must not include any spaces. Enter the new Password twice to confirm it.

Click the Save button when finished.

Click the Clear All button to clear all.

*Trabajo colaborativo en clase, realizado por :*

- Georgi Gladkihh Kalinin ([georgigladkihh@gmail.com](mailto:georgigladkihh@gmail.com))
- María Sánchez Guzmán ([amsanchezsetenil@gmail.com](mailto:amsanchezsetenil@gmail.com))
- Alejandro Lorenzo Vargas ([alexlorenzo777@gmail.com](mailto:alexlorenzo777@gmail.com))
- Antonio Luis Domínguez Lebrón ([antonioluisdl@gmail.com](mailto:antonioluisdl@gmail.com))