



EKSELANS BY ITS

USER MANUAL

IPC-S2

250017

SLAVE FOR EKOAX



V03

TABLE OF CONTENTS

Installation	4
Packaging and accessories	4
Hardware features.....	5
IPC-S2 Installation	6
IPC-S2 connection	6
Operating the IPC-S2	7
Prepare IPC-S2 for web management.....	7
Web Management Access	8
Web management interface.....	9
Introduction	9
Main menu.....	9
Status.....	10
Device information	10
Network Side Information	10
User Side Information	11
Remote Management Status.....	11
Network.....	12
Broadband Setup	12
LAN Setup	14
WLAN Setup	16
Remote Management	17
User Number Limit.....	17
Timer Setup	17
Security (seguridad)	18
Denial Service.....	18
URL Filtering	18
IP Filtering	19
MAC Filtering.....	19
Service.....	20
Port Forwarding	20
DDNS	20

UPNP Setup	21
Advance NAT	21
Telnet Server	22
IGMP	22
Policy Route	23
Policy DNS	23
System	24
System Log	24
Save/Upgrade Setup	25
Reboot	26
Admin Account Management	27
Diagnosis	27
Language	28
Installation Examples	29
Features	30

Installation

The internet user unit by coaxial, model IPC-S2 allows you to perform in combination with the main headend unit, model IPC-M2 and M3, a fast and secure internet installation through the coaxial cable.

In this chapter you will find the following information:

- Packaging and accessories of the IPC-S2.
- Hardware features of the IPC- S2.
- Installing the IPC-S2.
- Connect the IPC-S2.

Packaging and accessories

In the IPC packaging, in addition to the manual, the following components are included:



User unit



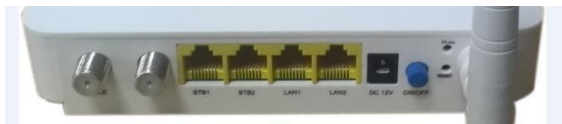
Ethernet cable



Power supply unit

Hardware features

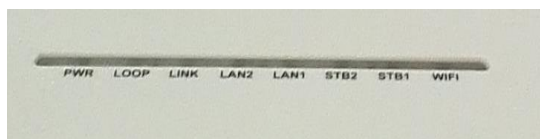
Rear panel



- **RF IN "CABLE"**: Radio frequency signal input.
- **RF OUT "TV"**: Radio frequency signal output.
- **LAN1 y LAN2**: Ethernet LAN ports to connect a PC. Can work in router and bridge mode
- **STB1 STB2**: Ethernet ports to connect a PC. The user's IP address can be obtained through a top-level device. Used for **IP TV**.
- **DC 12V**: Power supply connector.
- **ON/OFF**: On/off button.
- **Reset**: Reset button.

Front panel

The device has the following status LEDs:



- **POWER**: In **green**, it will indicate that the equipment is connected to the current.
- **LOOP**: On, it will indicate that there is some loop, in the network.
- **LINK**: In **green** with slight flickering, it is working properly. Off, the IPC-S2 is turned off or there is no communication with the headphone.
- **LAN1-2**: In **green**, the LAN port has established an Ethernet connection to another device (for example, a PC). With **flickering in green**, it's in the process of transmitting or receiving data. **Power off**, the IPC-S2 is turned off or there is no Ethernet connection to another device.
- **STB1-2**: In **green**, the LAN port has established an Ethernet connection to another device (for example, a PC). With **flickering in green**, it's in the process of transmitting or receiving data. **Power off**, the IPC-S2 is turned off or there is no Ethernet connection to another device.
- **WIFI**: In **green** it is working correctly. **Off**, the computer is turned off or there is no WiFi connection set.

IPC-S2 Installation

The user unit enables accessing the internet, either through a Wi-Fi connection or via connection to a PC to one of the LAN or STB ports of the equipment.

It is important to bear in mind that the range of the Wi-Fi network will depend on the location of this user unit. For best results, a series of recommendations is specified below in this regard:

1. Locate the IPC in the area/room where computers, tablets are located. The connection will improve if it is in the line of sight of this IPC user unit.
2. Attempt to locate the equipment far away from possible sources of interference, such as fans, Wireless security systems, microwaves, 2.4 GHz transmitters or cordless telephone base stations.
3. Likewise it is recommended to keep the equipment away from metal surfaces.

IPC-S2 connection

To connect this user unit, follow the steps below:

1. Connect the LAN port to a device (for example, a PC).
2. Connect the RF IN connector to the coaxial cable from the distribution network, which will be connected to the IPC-M head-end device.
3. Run power to the device through the supplied power supply.
4. Press the On/Off button on the rear panel to put into operation the IPC. The LED will flash green/red.

Operating the IPC-S2

Accessing the IPC-S2 slave device

This chapter explains how to access and configure the IPC-S2 slave after completing the wiring as explained in the previous chapter.

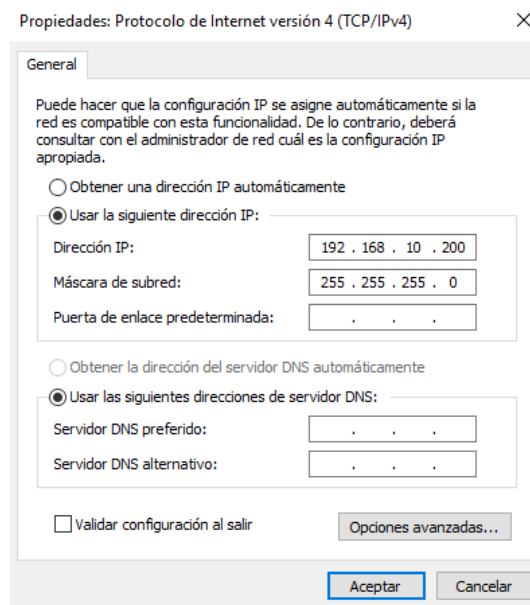
This chapter contains the following sections:

- Preparation for IPC-S2 web management
- Enter Web Management

Prepare IPC-S2 for web management

Prior to accessing the IPC it is important to verify that the connection between the equipment and PC is correct. It is recommended to follow the steps below:

1. Configuration of the IP address of the PC to 192.168.10.X(2-254), subnet mask 255.255.255.



2. Perform a "ping" to the IPC's IP address (by default 192.168.10.1). If the PC receives a correct response to the ping command, this will mean that the connection between the PC and the IPC is correct.

```

Simbolo del sistema
Microsoft Windows [Versión 10.0.18362.410]
(c) 2019 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Lab>ping 192.168.10.1

Haciendo ping a 192.168.10.1 con 32 bytes de datos:
Respuesta desde 192.168.10.1: bytes=32 tiempo=1m TTL=64
Respuesta desde 192.168.10.1: bytes=32 tiempo=1m TTL=64
Respuesta desde 192.168.10.1: bytes=32 tiempo=1m TTL=64
Respuesta desde 192.168.10.1: bytes=32 tiempo=1m TTL=64

Estadísticas de ping para 192.168.10.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
            (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\Lab>

```

Web Management Access

1. Open an internet browser and enter the following IP address: <http://192.168.10.1>. By clicking "Enter" will appear the login screen.



Username:

Password:

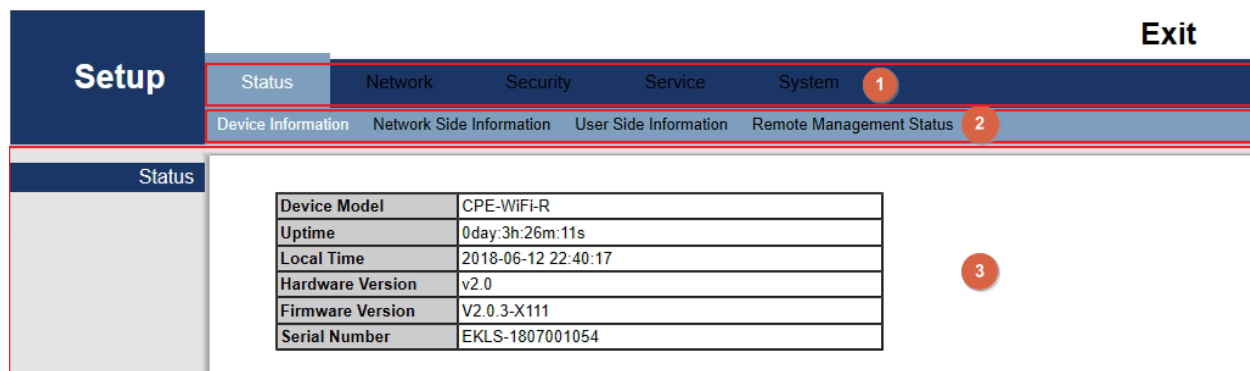
2. The credentials to access as an administrator are: Username: **admin**. Password: **admin**.
3. Having done so, press Enter to access the device management.

Note: it is possible to change the password from the web management interface.

Web management interface

The web management interface will allow for a quick configuration of different functions of the IPCs.

Introduction



The interface consists of three areas as shown in the previous image:

1. Main menu area
2. Sub menu area.
3. Area to show the results.

Main menu

- **Status:** Device information, Network Side Information, User Side Information, Remote Management Status.
- **Network:** Broadband Setup, LAN Setup, WLAN Setup, Move Device, Remote Management, User Number Limit, Time Setup.
- **Security:** Denial of Service, URL Filtering, IP Filtering, MAC Filtering.
- **Application:** ALG Setting, Dynamic DNS, UPnP, DMZ Setting, Port Forward, IGMP Setting.
- **Service:** Port Forwarding, DDNS, UPNP Setup, Advance NAT, Telnet Server, IGMP, Policy Route, Policy DNS.
- **System:** System Log, Save/Upgrade Setup, Reboot, Admin Account Management, Diagnosis, Manual Inform, Language.

The "Status" section includes submenus which displays different WAN and LAN connection values.

Click on the "Device information" section in order to access the following screen:

The model, functionality of the model in question, hardware version and software version will be displayed.

The menu will display the following network-related information:

ITS Partner O.B.S S.L · Av. Cerdanyola 79-81 Local C
08172 Sant Cugat del Vallés · Barcelona (Spain)
Phone: +34935839543 · info@ek.plus · www.ek.plus

The page will display the status of the WAN connection. Displays the name of the current WAN connection, connection type, connection status, default gateway, IP address obtained, subnet mask, preferred DNS1 and DNS2.

It will likewise display the connection values with the head-end, such as: attenuation, entry/exit, and noise levels.

User Side Information.

It will display different information such as Wi-Fi status, errors and packets sent and received from same, as well as the SSID status and encryption.

It will likewise display information as regards the LAN, the MAC of the slave or in the event of having a device connected to its IP and the errors in the packets sent and received.

Setup

Status

Network

Security

Service

System

Device Information

Network Side Information

User Side Information

Remote Management Status

Wireless Status

Wireless Status

Channel Number

Receives

Transmits

SSID Index

SSID Name

Auth Mode

Encryption

User Side Status

MAC Address

IP Address

CPE Type

IP Address

MAC Address

Status

Receives

Transmits

Network

The operating parameters of both the WAN, LAN or WLAN (Wi-Fi) can be configured and managed from this menu.

Broadband Setup

The Network is configured by default. A new network can be changed, deleted or added. Different WAN connections can be configured to offer various services to users.

The screenshot shows the 'Setup' menu with 'Network' selected. Under 'Network', 'Broadband Setup' is highlighted. The 'Network Setup' section displays a table with the following data:

Network Name	Port Mapping	Operation
1_INTERNET_R_VID_	lan1 lan2 wlan1	modify delete

Below the table is an 'Add' button.

In the event of changing or creating a new network, the following options are specified below:

The screenshot shows the 'Network Setup' configuration page. The options are as follows:

- VLAN Enable:
- VLAN ID: (1-4093)
- 802.1p: (0-7)
- Network Name:
- Service Mode:
- WAN Access Type:
- MTU: (1400-1500 bytes)
- DHCP Option Enable:
- DHCP Option60:
- Bind Port:
 - ☒ LAN1 ☒ LAN2 ☐ WLAN3 ☐ WLAN4
 - ☒ WLAN1 ☐ WLAN2

At the bottom are 'Save' and 'Reset' buttons.

Through this option, the WAN network settings are made. The WAN connection can function under "route" mode or "bridge" mode. A LAN or Wi-Fi port can be connected in the WAN connection in the Bind Port component.

- **VLAN Enable:**
 - **Enable:** Enable VLAN.
 - **Disable:** Disable VLAN.
- **VLAN ID:** The VLAN assigned.
- **802.1p:** A priority to the VLAN, with 1 being the lowest and 7 highest is assigned.
- **Network Name:**
 - **TR069:** The connection which is used for TR069.
 - **INTERNET:** The connection is used for INTERNET, and does not withstand TR069.
 - **TR069_INTERNET:** The connection is used for INTERNET and TR069.
 - **Other:** For other options.
- **Service mode:**
 - **Route:** When the connection is established in Router mode, the WAN IP can be obtained in three ways: DHCP, static or PPPoE. It is the default mode.
 - **Bridge:** It does not manage the IP, operates in a transparent manner by acquiring the DHCP from another router. By acting transparently, everything will remain within the network of the router which provides the service. If this operating mode is selected, the PC or any other device will obtain the IP address of a higher layer device after connection.
- **WAN Access Type:**
 - **DHCP:** Acquires dynamic IP. And if you choose DHCP, the router will automatically get the IP address from a higher layer device.
 - **Static IP:** We assigned an IP manually.

WAN Access Type:	Static IP
Ip Address:	172.1.1.1
Subnet Mask:	255.255.255.0
Default Gateway:	172.1.1.254

- **PPPoE:** Acquiring an IP via PPP protocol, a username and password will be assigned.

WAN Access Type:	PPPoE
PPPoEUser Name:	
PPPoEPassword:	

- **MTU:** Packet size.
- **DHCP Option Enable:** Enables an optional DHCP.
- **DHCP Option60:** By default 600831STB.
- **Blind Port:** Assignment of a port with the WAN service. The default WAN connection for all ports is in Router mode. If a new WAN connection is chosen in Bridge mode, a Router mode port can be assigned/unassigned. Different WAN connections can be configured to offer several services to users.

Note: all ports are defined by default in Router mode. If a connection is established in Bridge mode, the chosen port will be disconnected from the WAN. The WAN connection will be shared with all ports specified in router mode except those defined in Bridge mode.

It is necessary to select a connection type in the WAN connection configuration. And as mentioned earlier, one of three modes can be selected: static, DHCP and PPPoE depending on the application.

LAN Setup

This menu enables the configuration of the IP services of the LAN network, such as the DHCP.

The IPCs are preconfigured in router mode, to use private IP addresses in the section of the LAN, and to act as a DHCP server. The default configuration of the LAN router is:

- IP LAN: 192.168.10.1
- Subnet Mask: 255.255.255.0

These addresses are part of the range of private addresses for use in private networks and are available for most applications. If the network on which the IPC will be installed requires a different IP address system, it can be changed in the "LAN Settings" menu as shown in the following image.

The screenshot shows the 'Setup' menu with 'Network' selected. Under 'Network', 'LAN Setup' is chosen. The configuration fields are as follows:

- IP Address:** 192.168.10.1
- Subnet Mask:** 255.255.255.0
- DHCP Server:** Enable (dropdown menu)

Below these fields is a table for DHCP list configuration:

Network Type	Start IP	End IP	Lease Time(minutes)
STB	192.168.10.20	192.168.10.30	720
Phone	192.168.10.30	192.168.10.40	720
Camera	192.168.10.50	192.168.10.60	720
Computer	192.168.10.100	192.168.10.200	720

At the bottom, there is a 'Set DNS Manually' checkbox (checked) and two fields for DNS:

- DNS1:** 8.8.8.8
- DNS2:** 8.8.4.4

'Apply' and 'Reset' buttons are located at the bottom left of the configuration area.

Note 1: In the event of changing the LAN IP addresses on the router while it is connected through a browser, the router will be disconnected. It will then be necessary to open a new connection using the new IP address and to enter once again.

By default the IPC acts as a DHCP server. It assigns an IP, DNS server and the default Gateway to all PCs connected to the LAN network. The default IP address (192.168.10.1) is also the Gateway address. The IPC will assign the IP addresses to all connected PCs, selecting these addresses from a range of addresses specified in the "LAN Settings" screen.

DNS: Server which enables access to websites via their names. If the internet provider requires specific information on these servers, select this option and enter the IP addresses of the DNS servers.

Note 2: DHCP is the abbreviation for Dynamic Host Configuration Protocol, which automatically assigns IP addresses, subnet mask and default gateway to LAN users.

DHCP Server: Enable ▾

Network Type	Start IP	End IP	Lease Time(minutes)
STB	192.168.10.20	192.168.10.30	720
Phone	192.168.10.30	192.168.10.40	720
Camera	192.168.10.50	192.168.10.60	720
Computer	192.168.10.100	192.168.10.200	720

Set DNS Manually: ☒

DNS1:

DNS2:

Apply Reset

- **DHCP Server:** Enable/disable the DHCP function.
- **Start IP:** The IP address from which the DHCP server will commence providing IP addresses to network users.
- **End IP:** End address of the range of IPs supplied by the DHCP server.
- **Lease Time:** The time that a user is permitted to be connected through the IP address provided automatically. This enables the reassignment of IP addresses which are no longer in use.

WLAN Setup

In this section it is possible to activate / deactivate the WiFi network, define the wireless channels, type of operation.

- **Enable Wireless:** Enable / disable WLAN.
- **Band:** Wi-Fi protocol with which it is broadcasted.
- **Channel Width:** Channel bandwidth.
- **Control Sideband:** It cannot be configured.
- **Channel Number:** Set the working channel manually (selection of the proposed list), or set to automatic mode.
- **Data Rate:** Wi-Fi connection speed, automatic default.
- **Protection:** Wifi protection, by default disabled.
- **Short GI:** By default, enabled this option improves wifi network performance.
- **RF Output Power:** Wi-Fi power output.
- **SSID:** Identifies the "set" of services with a specific Wi-Fi network.
- **Hide SSID:** Tick this option to hide the SSID.
- **Encryption method:** Select the encryption type: None, WEP, WPA- PSK, WPA2 -PSK and Mixed WPA2/WPA -PSK. In the event of selecting an encryption method, it will be necessary to configure the identification method and password.

Remote Management

The protocol used by operators to remotely configure ADSL routers or cable modems can be enabled/disabled.

The screenshot shows the 'Setup' menu with 'Remote Management' selected. The 'Status' tab is active, displaying the following configuration options:

- TR069:** ☐ Disabled ☒ Enabled
- ACS:**
- URL:**
- User Name:**
- Password:**
- Periodic Inform Enable:** ☐ Disabled ☒ Enabled
- Periodic Inform Interval:**
- Connection Request:**
 - User Name:**
 - Password:**
 - Port:**

Buttons: [Apply] [Undo]

User Number Limit

Set a maximum user limit.

The screenshot shows the 'Setup' menu with 'User Number Limit' selected. The 'Status' tab is active, displaying the following configuration options:

- Mode:**

Buttons: [apply]

Timer Setup

The time can be configured in several ways. It is possible to do it manually. By default the NTP (Network Time Protocol) is not enabled in order to obtain the time automatically.

The screenshot shows the 'Setup' menu with 'System Time' selected. The 'Status' tab is active, displaying the following configuration options:

- Local Time:**
- Copy Computer Time:**
- Time Zone Select:**
- ☐ Automatically Adjust Daylight Saving
- ☒ Enable NTP client update
- Primary NTP Server:**
- Alternate NTP Server:**

Buttons: [Apply] [Reset] [Refresh]

Security

From this section the several types of security on the equipment can be configured.

Denial Service

The different types of protection can be selected By default: Dos Prevention, TCP/UDP PortScan, ICMP Smurf, Ping of Death,

Also, we can select packages per Second and degree of protection (Low/High).

The screenshot shows the 'Setup' menu with 'Security' selected. Under 'Security', 'Denial of Service' is chosen. The configuration options are:

- ☒ Enable DoS Prevention
- ☐ Whole System Flood: SYN
- ☒ TCP/UDP PortScan
- ☒ ICMP Smurf
- ☒ PingOfDeath

Additional settings include a text input for 'Packets/Second' (value: 100) and a dropdown for 'Sensitivity' (options: Low, High). Buttons for 'Select ALL', 'Clear ALL', and 'Apply' are at the bottom.

URL Filtering

Option which permits adding a filtering table for URLs. Click the "Add" button to add the rules to be established, then "Apply".

The screenshot shows the 'Setup' menu with 'Security' selected. Under 'Security', 'URL Filtering' is chosen. The configuration options are:

- ☒ Enable URL Filtering
- Mode: Black list

Below is a table for the 'Current Filter Table':

URL Address	Select

Buttons at the bottom include 'Add', 'Delete Selected', 'Delete All', 'Apply', and 'Reset'.

IP Filtering

The IP filtering can be enabled/disabled. Click the "Add" button to add the desired rules, then "Apply".

The screenshot shows the 'Setup' menu with 'Security' selected. Under 'Security', 'IP Filtering' is chosen. On the left sidebar, 'IP Filtering' and 'Ip Filter Table' are listed. The main content area has a checkbox 'Enable IP Filtering' which is checked. Below it, a section titled 'Current Filter Table:' contains a table with headers: 'Local IP Address', 'Protocol', 'Comment', and 'Select'. At the bottom of this section are buttons: 'Add', 'Delete Selected', 'Delete All', 'Apply', and 'Reset'.

MAC Filtering

The MAC filtering can be enabled/disabled. Click the "Add" button to add the desired rules, then "Apply".

The screenshot shows the 'Setup' menu with 'Security' selected. Under 'Security', 'MAC Filtering' is chosen. On the left sidebar, 'MAC Filtering' and 'MAC Filter Table' are listed. The main content area has a checkbox 'Enable MAC Filtering' which is checked. Below it, a section titled 'Current Filter Table:' contains a table with headers: 'MAC Address', 'Comment', and 'Select'. At the bottom of this section are buttons: 'Add', 'Delete Selected', 'Delete All', 'Apply', and 'Reset'.

Service

In the "service" section ports can be redirected or different parameters configured such as DDNS, UPNP Setup, among others.

Port Forwarding

The destination source address and origin source ports to redirect ports can be added.

The screenshot shows the 'Setup' menu with 'Service' selected. Under 'Service', 'Port Forwarding' is chosen. The 'Port Forwarding Table' is empty. To the right, there are input fields for configuring a new rule: Name, Local IP, Inner Port, Remote IP, Outer Port, Protocol (set to 'Both'), Status (set to 'Disable'), and a 'Save' button.

DDNS

A Dynamic Domain Name System can be established if registered on the websites of the different providers and following the necessary steps.

The screenshot shows the 'Setup' menu with 'Service' selected. Under 'Service', 'DDNS' is chosen. The 'Enable DDNS' checkbox is unchecked. Below it, there are input fields for 'Service Provider' (set to 'DynDNS'), 'Domain Name' (set to 'host.dyndns.org'), 'User Name', and 'Password'. There are 'Apply' and 'Reset' buttons at the bottom.

UPNP Setup

It allows us to activate the UPnP protocol. Universal Plug and Play (UPnP) is a network protocol that allows compliant devices to automatically set port forwarding rules for themselves. Whatever device that communicate with each other and share data over your network.

The screenshot shows the 'Setup' menu with tabs for Status, Network, Security, Service, and System. Under the 'Service' tab, there are sub-tabs: Port Forwarding, DDNS, UPNP Setup, Advanced NAT, Telnet Server, IGMP, Policy Route, and Policy DNS. The 'UPNP Setup' sub-tab is selected. On the left sidebar, 'UPNP Setup' is highlighted. The main content area has the heading 'UPNP Setup'. It contains a checkbox labeled 'Enable UPnP' which is checked. Below it is a label 'Interface' followed by a dropdown menu showing '1_INTERNET_R_VID_'. At the bottom are 'Apply' and 'Reset' buttons.

Advance NAT

Enables and disables different protocols.

The screenshot shows the 'Setup' menu with tabs for Status, Network, Security, Service, and System. Under the 'Service' tab, there are sub-tabs: Port Forwarding, DDNS, UPNP Setup, Advanced NAT, Telnet Server, IGMP, Policy Route, and Policy DNS. The 'Advanced NAT' sub-tab is selected. On the left sidebar, 'ALG Setup' and 'DMZ Setup' are visible. The main content area has the heading 'Advanced NAT'. It contains a list of checkboxes: 'Enable Web Server Access on WAN', 'Enable Ping Access on WAN', 'Enable IPsec pass through on VPN connection', 'Enable PPTP pass through on VPN connection', 'Enable L2TP pass through on VPN connection', 'Enable H.323', 'Enable FTP', and 'Enable SIP'. All these checkboxes are checked. Below this list is an unchecked checkbox labeled 'Enable DMZ'. Under 'Enable DMZ' is a label 'DMZ Host IP Address:' followed by an empty text input field. At the bottom are 'Apply' and 'Reset' buttons.

Telnet Server

Enables Telnet access to the device.

The screenshot shows the 'Setup' menu with 'Service' selected. Under 'Service', 'Telnet Server' is highlighted. The configuration page for 'Telnet Server' is displayed, showing a checkbox for 'Enable Telnet Server' which is checked. Below the checkbox is an 'Apply' button.

IGMP

Enables to activate as IGMP proxy and IGMP Snooping for multicast package management.

The screenshot shows the 'Setup' menu with 'Service' selected. Under 'Service', 'IGMP' is highlighted. The configuration page for 'IGMP' is displayed, showing two checkboxes: 'Enable IGMP Proxy' (checked) and 'Enable IGMP Snooping' (unchecked). Below the checkboxes are 'Apply' and 'Reset' buttons.

Policy Route

These are team policy-based routing rules. If necessary, we can add to manually configure or modify existing ones.

The screenshot shows the 'Setup' menu with 'Service' selected. Under 'Service', 'Policy Route' is highlighted. The 'Policy Route Table' is displayed on the left. The main table has the following data:

IP Address	Subnet Mask	Service Mode	Select
10.43.0.0	255.255.0.0	VOD	☐
10.32.0.0	255.255.0.0	TR069	☐

Below the table are buttons: Add, Delete Selected, Delete All, Apply, and Reset.

Policy DNS

These are policy-based DNS rules for the computer. We can add if necessary to manually configure or modify existing ones.

The screenshot shows the 'Setup' menu with 'Service' selected. Under 'Service', 'Policy DNS' is highlighted. The 'Policy DNS Table' is displayed on the left. The main table has the following data:

Domain Name	Service Mode	Select
sxgdtcms.com	TR069	☐
homedev.com	TR069	☐
hitv.com	VOD	☐
sxgdvod.cn	VOD	☐
sxgdtcms.cn	VOD	☐
sxbctv.com	VOD	☐
ott.suning.com	VOD	☐

Below the table are buttons: Add, Delete Selected, Delete All, Apply, and Reset.

System

System maintenance menu that includes the options: System Log, Save/Upgrade Setup, Reboot, Admin Account Management, Diagnosis, Manual Inform, Language.

System Log

The "Enable Log" option can be selected to enable / disable the device's action log, including emergency indications, alerts, critical points, errors, warnings. In total 8 categories can be selected depending on the operation of the device.

The screenshot shows the 'System Log' configuration page within the 'Setup' menu. The page has a dark blue header with 'Setup' and a sub-header with 'System Log', 'Save/Upgrade Setup', 'Reboot', 'Admin Account Management', 'Diagnosis', 'Manual Inform', and 'Language'. The main content area is titled 'System Log' and contains the following options:

- ☐ Enable Log
 - ☐ system all
 - ☐ wireless
 - ☐ DoS
- ☐ Enable Remote Log
- Log Server IP Address:

Below these options is an 'Apply' button. At the bottom of the page are 'Refresh' and 'Clear' buttons.

Save/Upgrade Setup

From this tab a backup and reload (Backup file/Restore file), perform a default reset "Reset router to defaults:" or update the "Firmware image" system can be carried out.

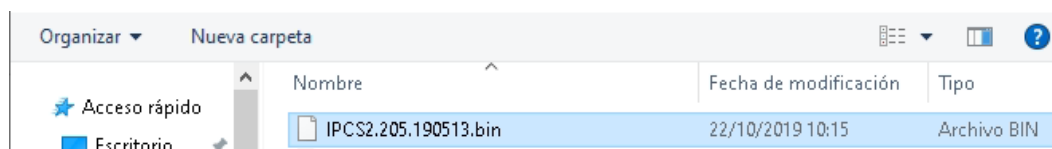
Also, this menu will show us the current version installed now, in our case the V2.0.5-X111.

To upgrade we follow the next steps:

1. Click



2. Select the file



3. Click Upload

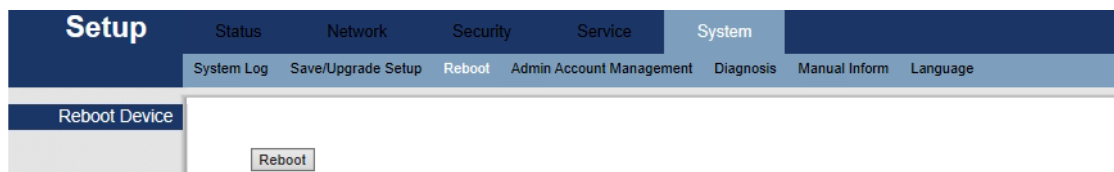


Then It will appear that the system is loading, we just have to wait for the process to finish. Be careful not to disconnect the device or leave it without supply voltage.



Reboot

This option enables a device reset. To that end click the "Reboot" button which will appear by selecting this option.



Admin Account Management

Team management can be done with two different levels of access and therefore two different users. Choose the user in question and assign/modify the access keys for each of them. Also, is possible to add new users.

With **administrator** level we will have all **privileges** meanwhile as a user does **not**.

ID	User name	User permissions	Password	New Password	Confirm new password	Operation
1	admin	Administrator				Modify Delete
2	useradmin	Administrator				Modify Delete
+		Administrator	+			Add

Diagnosis

A web address can be pinged in order to verify that the internet is available on the equipment. **Select a Google page** given that the webpage which appears by default does not function for web security..

Diagnose Mode: Ping

Interface: 1 INTERNET_R_VID

Destination IP address or Host Name: www.google.es

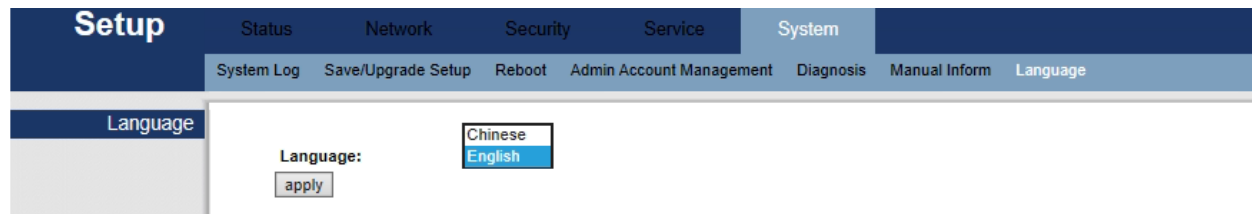
Apply

Diagnose Result:

```
64 bytes from 172.217.16.227: seq=0 ttl=53 time=10.000 ms
64 bytes from 172.217.16.227: seq=1 ttl=53 time=20.000 ms
64 bytes from 172.217.16.227: seq=2 ttl=53 time=20.000 ms
64 bytes from 172.217.16.227: seq=3 ttl=53 time=10.000 ms
64 bytes from 172.217.16.227: seq=4 ttl=53 time=20.000 ms
--- www.google.es ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
```

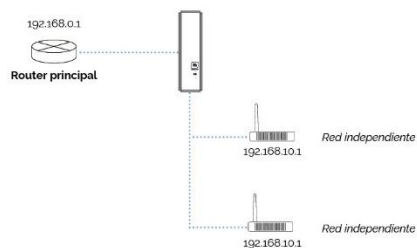
Language

Two languages can be selected, that is, English or Chinese.



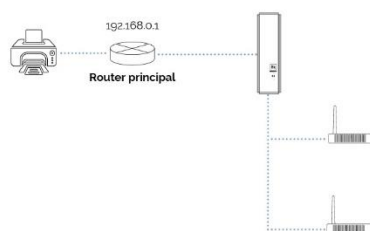
Installation Examples

Instalación 1: Modo Router



* Los equipos IPC no ven que hay en la red principal 192.168.0.1. Tampoco entre ellos

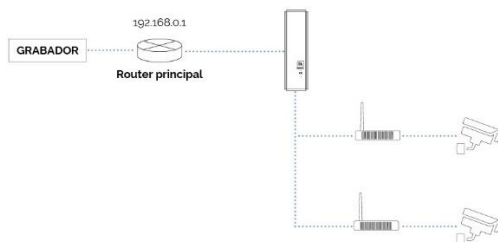
Instalación 2: Modo Bridge



* Los equipos están en la red principal, viendo si hay otros dispositivos. Pueden utilizar la impresora.

Nota: Entre ellos no pueden ver que hay conectado

Instalación 3: Modo Bridge con cámaras



Nota: Para su correcto funcionamiento, el grabador ha de estar en el router principal. La comunicación entre equipos de esclavo-esclavo no es posible

Features

Property	Description
Consumption	<8W
Power supply	12V/1A
Dimensions	160×120×32 mm
Working temperature	0°C~50°C
Storage temperature	-40°C~85°C
Moisture	10%~90% non-condensing
Storage humidity	10%~90% non-condensing