INTERNET

UTILIZACIÓN DEL SERVICIO – ROUTERS

CISCO RV042 – INSTRUCTIVO DE CONFIGURACIÓN

IPLAN



ÍNDICE

1.	Introduc	ción	Pág. 03
2.	Configu	ración Básica	Pág. 03
	2.1	Ingresando a la Configuración web del Router	Pág. 03
	2.2	Resumen del Sistema	Pág. 04
	2.3	Configuración de Red	Pág. 04
	2.4	Acceso Web	Pág. 06
	2.5	Fecha y Hora	Pág. 06
	2.6	Servidor DHCP	Pág. 07
3.	Configu	ración avanzada	Pág. 08
	3.1	Firewall	Pág. 08
	3.2	Redirección de puertos	Pág. 09
	3.3	Configuración de Dual WAN	Pág. 11
		3.3.1 Balanceo de Carga	Pág. 11
	3.4	Configuración de QoS	Pág. 12



1. INTRODUCCIÓN

El presente instructivo tiene como objetivo guiarte a configurar un **Router Cisco RV042**, que esté bajo modalidad venta o lo hayas adquirido a un tercero.

Aquellos equipos que no están en modalidad de venta ni fueron adquiridos a terceros, es decir equipos bajo la modalidad de servicio, son administrados por **IPLAN**. Es importante que bajo esta modalidad no realices modificaciones en los mismos ni uses el procedimiento de **Factory Reset** (volver a valores de fábrica), ya que la reconfiguración del mismo tendrá costo.

Los parámetros de configuración que mostraremos a lo largo del instructivo pueden ser aplicables a otros modelos de Routers de la misma u otras marcas según el caso.

Tené presente que el Router **Cisco RV042** anteriormente era comercializado por **Linksys**, por lo que puede sucederte que las imágenes mostradas en este instructivo no coincidan si contás con el mismo Router pero en versión Linksys. A pesar de esto, la mayoría de las secciones y opciones a configurar son exactamente las mismas, por más que cuenten con una apariencia gráfica distinta.

Para garantizar que el equipo quede bien configurado y no surjan inconvenientes luego de la implementación, te recomendamos que previamente el mismo este reseteado a valores de fábrica.

Para más información sugerimos la lectura de la documentación del fabricante.

2. CONFIGURACIÓN BÁSICA

2.1 INGRESANDO A LA CONFIGURACIÓN WEB DEL ROUTER

Para configurar el **Router** en cuestión, el procedimiento debe realizarse mediante una página Web interna del dispositivo para tal fin, utilizando el número de **Dirección IP** correspondiente al Router.

En caso de que el **Router** ya se encuentre configurado, te recomendamos consultar el manual del mismo para realizar un procedimiento de **Factory Reset** (volver a valores de fábrica el Router)

Asumiendo que el **Router** se encuentra reseteado a valores de fábrica o bien que nunca fue configurado anteriormente, la **Dirección IP Privada** correspondiente al mismo será **192.168.1.1**.

Para la configuración del Router vía web, seguí los pasos a continuación:

- Abrí un navegador web e ingresá la dirección web del Router. Ejemplo: <u>http://192.168.1.1</u>
- Luego, autentícate con el Usuario y Clave de Administrador solicitados por la página. Los datos de usuario y contraseña por defecto son:
 - Usuario: admin
 - o Clave: admin
- Presioná el botón Login para confirmar.

cisco	Router	Username:	admin	1
		Password:	•••••	•
		2	Login	



2.2 RESUMEN DEL SISTEMA

La pantalla inicial de la configuración Web del Router será similar a la imagen a continuación.

En ella observarás un resumen de todos los datos de IP configurados, como así también el estado de todas las interfaces / puertos del equipo.

small Business cisco RV042 10	0/100 4-P	ort VPN	Router	-			admin Logout	About	Help
System Summary Setup DHCP	System S System Inform	ummary							
 System Management 	Serial Numbe	Serial Number : NKS11073418 Firmware Version :			e Version :	v4.0.0.07-tm (Aug 1	9 2010 19:19:50)		
Port Management	PID VID :	F	RV042 V03	Firmwa	e MD5 Checksum :	5a58bcbb6358a78a	a2b40cbf50fc4a1f	0	
Firewall	LAN IP / Subr	net mask :	192.168.0.1/255.255.255.0) Working	Mode :	Gateway			
Cisco ProtectLink Web	System Up Ti	me:	18 Days 5 Hours 42 Minu	tes 30 Seconds (N	ow : Fri May 11 2012	2 10:13:59)			Ξ
VPN								_	
▶ Log	Cisco P	rotectLink				Go buy Registe	r Activate		
Wizard									
	Configuration	uideline to re-	configure the router, you r	nay launch wizard.	Setup Wizard				
	Port Statistic	s							
	Port ID	1	2	3	4	Internet	DMZ/Internet	t	
	Interface		L	AN		WAN1	WAN2		
	Status	Connected	d Connected	Connected	Enabled	Connected	Enabled		
WAN Status WAN1 WAN2									
	•			III				•	
WAN Status WAN1 WAN2 VID Clisco Systems. Inc. All rights reserved.					•				

2.3 CONFIGURACIÓN DE RED

Para comenzar a configurar el Router, ingresá a la sub-sección Network dentro de la sección Setup.

En caso de necesitar modificar la Dirección IP Privada del Router, seguí los pasos a continuación:

- Ingresá la dirección IP en Device IP Address y luego su máscara de subred en Subnet Mask
- Hacé un click en el botón Save y luego volvé a ingresar al equipo con la nueva Dirección IP Privada

System Summary	Matuali			
▼ Setup	Network			
Network	Host Name :	Router-Empresa	(Required by some ISPs)	
Password	Demain Name :	mideminie eem er	(Dequired by sema IODs)	
Time	Domain Name .	midominio.com.ar	(Required by some ises)	
DMZ Host				
Forwarding	LAN Setting			
UPnP	MAC Address	C8:9C:1D:5B:5D:30		
Une-to-Une NAT				
Dynamic DNS	Device IP Address :	192.168.1.1		
Advanced Routing	Subnet Mask :	255.255.255.0 🔻		
▶ DHCP	Multiple Subnet :	Enable Add/Edit		
System Management				
Port Management	WAN Setting			
Firewall	Interface	Connection Type	Configuration	
Cisco ProtectLink Web	Internace	Connection Type	Configuration	
▶ VPN	WAN1	Static IP		
▶ Log	WAN2	Obtain an IP automatically		
Wizard				
	DMZ Setting			
		~		
	Enable DMZ	2		
	Save Cano	cel		



Dentro de la misma sub-sección, deberás definir el **Direccionamiento IP Público** provisto por **IPLAN**. Para esto, seguí los pasos a continuación:

• Hacé un click en el ícono del papel del renglón WAN1 (ver imagen).

System Summary Setup	Network						
Network	Host Name :	Router-Empresa	(Required by some ISPs)				
Password Time	Domain Name :	midominio.com.ar (Required by some ISPs)					
Forwarding	LAN Setting						
One-to-One NAT	MAC Address :	C8:9C:1D:5B:5D:30					
MAC Address Clone	Device IP Address :	192.168.1.1					
Dynamic DNS Advanced Routing	Subnet Mask :	255.255.255.0 🔻					
DHCP	Multiple Subnet :	Enable Add/Edit					
System Management							
Port Management	WAN Setting						
Firewall	Interface	Connection Type	Configuration				
 Cisco ProtectLink Web 	WAN1	Static IP					
VPN	WAN2	Obtain an IP automatically					
▶ Log	11/11/2	obtain an in automatically	2				
Wizard	DMZ Setting						
	Enable DMZ						
	Save Can	cel					

- Completá los datos a continuación:
 - WAN Connection Type: Static IP
 - o Specify WAN IP Address: Dirección IP Pública otorgada (Ej: 200.200.200.133)
 - o Subnet Mask: Mascara de subred de la IP otorgada. (Ej: 255.255.255.252)
 - o Default Gateway Address: Puerta de enlace otorgada. (Ej: 200.200.200.134)
 - o DNS Server (Required): Ingresá 200.69.193.1 y 190.210.156.1 respectivamente.
- Hacé un click en Save en esta pantalla y en la siguiente para guardar los cambios.

System Summary Setup	Network				
Network	Edit WAN Connection				
Password Time	Interface :	WAN1			
DMZ Host	WAN Connection Type :	Static IP	•		
Forwarding UPnP	Specify WAN IP Address :	200.200.200.133			
One-to-One NAT	Subnet Mask :	255.255.255.252		1	
MAC Address Clone Dynamic DNS	Default Gateway Address :	200.200.200.134		1	
Advanced Routing	DNS Server (Required) 1 :	200.69.193.1			
DHCP	2 :	190.210.156.1			
System Management	мти.			500	
Port Management		Auto	Manual 1	500	Dytes
Firewall	Save Cancel				
 Cisco ProtectLink Web 					
VPN					
▶ Log					
Wizard					



2.4 ACCESO WEB

Al finalizar la configuración de red, ingresá a la sub-sección **Password** dentro de la sección **Setup**. Aquí podrás definir los datos de acceso al Router. Para esto, especificá los siguientes parámetros:

- Old Password: Escribí la contraseña actual
- New Username / Confirm New Username: Escribí un nuevo usuario.
- New Password / Confirm New Password: Escribó una nueva contraseña para el usuario definido.
- Realizá un click en el botón Save para guardar los cambios.

System Summary Setup	Password		
Network	Username :	admin	
Password	Old Password :		
Time DMZ Host	New Username :	admin	
Forwarding UPnP	Confirm New Username :	admin	2
One-to-One NAT	New Password :	•••••	
MAC Address Clone Dynamic DNS	Confirm New Password :		
Advanced Routing	Minimum Password Complexity :	Enable	
DHCP	Password Strength Meter :		
 System Management 			
Port Management	Password Aging Enforcement :	Disable Change the password after	
Firewall		Days	
Cisco ProtectLink Web	Save Cancel		
VPN			
▶ Log	<u> </u>		
Wizard			

2.5 FECHA Y HORA

Una vez realizados los pasos anteriores, ingresá a la sub-sección **Time** dentro de la sección **Setup**. Aquí podrás definir la fecha y hora del Router. Para esto, definí los siguientes parámetros:

- Elegí la opción Set the local time using Network Time Protocol (NTP) automatically
- Seleccioná Buenos Aires (GMT-3:00) en Time Zone
- Definí time-a.nist.gov en NTP Server
- Hacé un click en el botón Save para guardar los cambios.

System Summary Setup	Time
Network	Set the local time using Network Time Protocol (NTP) automatically
Password	Set the local time Manually
Time	
DMZ Host	
Forwarding UPnP	Time Zone : 3 Buenos Aires (GMT-3:00)
One-to-One NAT	Daylight Savings Time : 📃 Enabled
MAC Address Clone	Shed Data i
Dynamic DNS	Statt Date . (film.dg)
Advanced Routing	End Date : (mm.dd)
DHCP	NTP Server : time-a nist dov
 System Management 	
Port Management	Save Cancel
Firewall	
Cisco ProtectLink Web	
VPN	
▶ Log	
Wizard	



2.6 SERVIDOR DHCP

El **Servidor DHCP** permite a una PC conectada a la red, adquirir automáticamente una **Dirección IP** y el resto de los parámetros para poder navegar (Mascara de Subred, Puerta de Enlace, DNS, etc)

Para poder configurarlo, ingresá en la sub-sección **DHCP** Setup dentro de la sección **DHCP**. Aquí podrás definir un Servidor DHCP junto con el rango de Direcciones IP que éste asignará (Pool)

Para configurar el Servidor DHCP, seguí los pasos a continuación:

- Tildá la opción Enable DHCP Server
- Definí cuánto tiempo durará una Dirección IP asignada antes de renovarse, en Client Lease Time.
- Especificá el **Rango de Direcciones IP** (Pool de IPs) a otorgar de forma automática. El rango debe estar dentro del segmento de red del Router y no debe superponerse con **Direcciones IP Estáticas**.

System Summary		
Setup	DHCP Setup	
▼ DHCP	C Enable DHCP Server	
DHCP Setup DHCP Status	DHCP Relay	
 System Management 	Evnamic IP	
Port Management		
Firewall	Client Lease Time : 1440 Minutes	
Cisco ProtectLink Web	Range Start : 192.168.0.200 2	
VPN	Bases End : 100 100 0 254	1
▶ Log	Kaige Eliu . 192.108.0.234	
Wizard	Statis ID	
	Stauc IP	
	Show unknown MAC addresses	
	Static IP Address :	
	MAC Address :	
	Name :	
	Enable :	
	Add to list	
	•	
	٠ () () () () () () () () () (

- Adicionalmente definí los Servidores DNS que se asignarán automáticamente a las PC. Completá 200.69.193.1 y 190.210.156.1 en DNS Server
- Hacé un click en el botón Save para guardar los cambios.

System Summary		······································	n.
 Setup 	DNS		
▼ DHCP	r		
DHCP Setup	DNS Server (Required) 1 :	200.69.193.1	
DHCP Status	2 :	190.210.156.1	
 System Management 	L		
Port Management	WINS		
Firewall			
Cisco ProtectLink Web	WINS Server :	0.0.0	
VPN	DNS Local Database		
▶ Log	DNS Local Database		
Wizard	Host Name :		
	IR Address :		
	In Address .		
		Add to list	
		A	
		-	
		Delete Add New	
	Save Cancel		÷

IPLAN | iplan.com.ar | NSS S.A. Reconquista 865 | C1003ABQ | Buenos Aires | Argentina Tel: 54-11-5031-6300 / Fax: 54-11-5031-6301

IPLAN

3. CONFIGURACIÓN AVANZADA

3.1 FIREWALL

Es posible habilitar el Firewall que viene incorporado en el Router, a fin de reforzar la seguridad contra usuarios no autorizados que intenten ingresar desde Internet hacia tu red.

Para esto, ingresá a la sub-sección General dentro de la sección Firewall. Seguí los pasos a continuación:

- Configurá los siguientes parámetros:
 - Firewall: Enable (Esto habilitará el resto de las opciones)
 - o SPI (Stateful Packet Inspection): Enable
 - o DoS (Denial of Service): Enable
 - **Block WAN Request**: Enable (Evita que el Router responda pings desde fuera de la red)
 - **Remote Management**: Disabled (Opcionalmente en Enable precisás acceso remoto al router)
 - **HTTPS**: Enable (Aumenta la seguridad en los ingresos al router usando HTTPS)
 - Multicast Passthrough: Disable
- Hacé un click en Save para guardar los cambios

NOTA: Si utilizás **HTTPS**, cada vez que quieras ingresar al **Router**, deberás hacerlo utilizando una dirección del siguiente formato: <u>https://192.168.1.1</u>, asumiendo que **192.168.1.1** sea la IP del **Router**

System Summary	Conorol					
Setup	General					
DHCP	Firewall :	Enable	Disable			
 System Management 	ODI (Otatati Da skut la sa stian) i	0				
Port Management	SPI (Statelul Packet Inspection) .	Enable	Disable		2	
▼ Firewall	DoS (Denial of Service) :	Enable	Disable			
General Access Rules	Block WAN Request :	• Enable	🔘 Disable			
Content Filter	Remote Management :	Enable	Oisable	Port : 8080		
 Cisco ProtectLink Web 	HTTPS :	Enable	O Disable			
VPN	Multicast Passthrough :	C Enable	Disable			
▶ Log			0 010000			
Wizard	Restrict Web Features					
	Block :	🔲 Java				
		Cookies				
		ActiveX				
		Access to H	HTTP Proxy Servers			
	Don't block Java/ActiveX/Cookies	s/Proxy to Trusted	I Domains			
	Save Cancel					

La mayoría de las opciones descritas anteriormente tienen como objetivo proteger a nuestra red frente ataques externos.

Para el caso de la opción **Remote Management**, que permite que un usuario pueda acceder desde Internet a la configuración del Router, recomendamos deshabilitarlo. Por otro lado, también sugerimos que las opciones **DoS** y **Block WAN Request** estén habilitadas por motivos de seguridad.

Excepcionalmente podemos solicitarte habilitar/deshabilitar alguna de estas opciones temporalmente ante una solicitud de asistencia técnica a **IPLAN**. De esta manera, ante un inconveniente, podremos realizar las pruebas que sean necesarias a fin de verificar rápidamente el incidente.



3.2 REDIRECCIÓN DE PUERTOS

Para realizar redirecciones de puertos, ingresá a la sub-sección UPnP dentro de la sección Setup.

Un ejemplo de aplicación para la redirección de puertos es contar con un servidor un **Servidor Web** dentro tu **Red Interna**, y que sea necesario que redirigir el puerto **80** de ese servidor para hacerlo visible desde internet.

Otro caso es el de los **Teléfonos IP**, donde podrás hacer una redirección para ver la página de configuración de estos desde Internet. Generalmente te solicitamos esto a la hora de brindarte soporte de forma remota sobre **Teléfonos IP** del servicio de **Central Virtual IPLAN**

UPnP (Universal Plug and Play) hace esto de forma automática para ciertas aplicaciones. Para activarlo, elegí **Yes** en **UPNP Function**. Para una redirección manual, seguí los pasos a continuación:

System Summary Setup	UPnP			
Network Password	UPnP Function :	• Yes O No		
Time DMZ Host	Service :	DNS [UDP/53~53]		
Orne-to-One NAT MAC Address Clone Dynamic DNS Advanced Routing	Name or IP Address : Enable :	Service Management 2		
> DHCP		Add to not		
System Management			^	
Port Management				
Firewall				
Cisco ProtectLink Web				
VPN				
▶ Log			-	
Wizard		Delete Add New		
	View Save	Cancel		

• Realizá un click en el botón Service Management

Especificá un nombre para el servicio, el tipo de protocolo (TCP, UDP o ambos), puerto externo e interno.
 Para el caso de una Redirección de Puertos para un Teléfono IP, tomá como ejemplo la imagen:

Service Manageme	nt - Mozilla Firefox 📃 🗖 💌
http://200.69.253.	233:8080/service1.htm 🟠
Service Name :	Telefono-1
Protocol :	
External Port :	60001
Internal Port :	80
	Add to list 2
DNS [UDP/63-53] FTP [CP/21-21] HTTP Secondary [CP/8 HTTPS [CP/443-443] HTTPS ICP/443-443] HTTPS UDP/89-89] MAP [CP/143-143] NNTP [CP/143-143] SMTP [CP/143-143] SMTP [CP/143-143]	1080-8080] :≡ :≈ :≈
	Delete Add New
OK Cancel	Close
Listo	н.



• Ahora el servicio aparecerá en la lista junto con el resto. Clickeá en el botón OK para guardar los cambios.



- Ahora que el servicio figura en la lista junto con el resto, seleccionarlo en el combo-box Service
- Definí la Dirección IP Privada de la PC al cual se redirigirán los puertos en Name or IP Address. Siguiendo el ejemplo mencionado anteriormente, esta Dirección IP Privada será la del Teléfono IP en cuestión.
- Tildá la opción Enable y hacé un click en Add to list.

System Summary Setup	UPnP
Network Password	UPnP Function : O Yes O No
Time DMZ Host Forwarding Unre One-to-One NAT MAC Address Clone Dynamic DNS Advanced Routing DHCP	Service : Telefono 1 (TCP/60001-80) Service Management Name or IP Address : 192.168.0.106 Enable : Add to list Add to list
DHCP System Management Port Management Firewall Cisco ProtectLink Web VPN Log	
Wizard	Delete Add New
	View Save Cancel
System Summary Setup	UPnP
System Summary Setup Network Password	UPnP UPnP Function : O Yes O No
System Summary Setup Network Password Time DMZ Host Forwarding	UPnP UPnP Function : • Yes • No Service : Telefono 1 [TCP/60001~80] • Service Management • Service Management
System Summary	UPnP UPnP Function : Yes No Service : Telefono 1 (TCP/60001-80) Service Management Name or IP Address : 192.168.0.106
System Summary	UPnP UPnP Function : Yes No Service : Telefono 1 (TCP/60001-80) Service Management Name or IP Address : 192.168.0.106 Enable : Unate
System Summary	UPnP UPnP Function: Yes No Service: Telefono 1 (TCP/60001-80) Service Management Name or IP Address: 192.168.0.106 Enable: Update Update Teleform 1 (TCP/60011-80)=102.168.0.106
System Summary System Summary System Summary Network Password Time DMZ Host Forwarding Unne: One-to-One NAT MAC Address Clone Dynamic DNS Advanced Routing DHCP System Management Firewall Cisco ProtectLink Web VPN Log	UPnP UPnP Function : Yes No Service : Telefono 1 (TCP/60001-80) Service Management Name or IP Address : 192.168.0.106 Enable : Update Telefono 1 (TCP/60001-80)>192.168.0.106
System Summary	UPnP UPnP Function : Yes No Service : Telefono 1 [TCP/60001-80] Service Management Name or IP Address : 192 168 0.106 Enable : Update Telefono 1 [TCP/60001-80]->192 168 0.100 Delete Add New

• Hacé un click en el botón Save para guardar los cambios



3.3 CONFIGURACIÓN DE DUAL WAN

El Router Cisco RV042 viene preparado para poder utilizar dos conexiones a Internet. Por este motivo, cuenta con dos puertos Ethernet destinados a ello: **WAN1** y **WAN2**, siendo WAN1 utilizada para la conexión de Internet de **IPLAN** y WAN2 para una conexión de backup.

En pasos anteriores, hemos configurado WAN1 para usar estáticamente lo datos de IP otorgados por IPLAN, mientras que WAN2 quedo en su valor por defecto, que es adquirir una dirección IP de forma automática (DHCP).

Esta configuración es válida para la mayoría de conexiones de otros ISP. Sin embargo, si es necesario realizar algún cambio bastará con que apliques los mismos pasos vistos anteriormente, pero esta vez sobre **WAN2**, en la sub-sección **Network** dentro de la sección **Setup**.

3.3.1 BALANCEO DE CARGA

Para poder definir el comportamiento de ambas conexiones, ingresá a la sub-sección **Dual WAN** dentro de la sección **DHCP**.

Casos de aplicación

• Si querés utilizar el Router para Internet y Central Virtual o algún otro servicio de telefonía provisto por IPLAN, deberás utilizar la opción Smart Link Backup: Primary WAN, con WAN1 definida como primaria.

El motivo de esta configuración, es que las líneas de Central Virtual se registran utilizando una determinada IP Pública que no debe modificarse, por lo que no podrás usar balanceo de carga.

Si especificarás la opción **Load Balance**, la telefonía no funcionaría correctamente ya que la mitad de la información viaja por una IP pública y la otra mitad por la otra, no pudiendo establecer correctamente las señalizaciones y las comunicaciones.

• Si querés utilizar el Router solamente para Internet y no para utilizarlo en conjunto con Central Virtual o algún otro servicio de telefonía provisto por IPLAN, podrás utilizar la opción Load Balance (Auto Mode) permitiendo aprovechar el ancho de banda de hasta dos conexiones en simultáneo.

Para ambos casos, realizá un click en Save luego de haber definido la opción correspondiente.

System Summary	Dual WAN
Setup	
► DHCP	
 System Management 	Smart Link Backup: Primary WAN WAN1 - (Specify which WAN is Primary, the other one will be backup)
Dual WAN	C Load Balance (Auto Mode)
Bandwidth Management	Δ
SNMP	Interface Setting
Discovery-Bonjour	interface setuing
Eactory Default	Interface Mode Configuration
Firmware Upgrade	WAN1 Auto 📝
Restart	WAN2 Auto
Backup and Restore	
Port Management	Save Cancel
Firewall	
Cisco ProtectLink Web	3
VPN	
▶ Log	
Wizard	



3.4 CONFIGURACIÓN DE QoS

En caso en que la conexión a Internet deba utilizarse tanto para telefonía como para Internet, como ocurre con el servicio de **Central Virtual IPLAN**, es necesario que configures calidad de servicio **QoS** (Quality of Service) a fin de priorizar el tráfico de telefonía por sobre el tráfico de datos.

Esto evita que la telefonía se vea afectada cuando hay gran consumo de Internet, ya que el **Router** le da menos prioridad al tráfico de datos, pudiendo mantener la calidad en la Telefonía.

Para definir estas cuestiones, ingresá a la sub-sección **Bandwidth Managment** dentro de la sección **System Managment**. Seguí los pasos a continuación:

- Definí el ancho de banda de bajada y subida para ambas conexiones, expresada en Kbit/sec. Para el caso de 10 megabits simétricos, el valor que deberás utilizar es 10240 por ejemplo.
- Asegurate de que esté configurada la opción Priority en lugar de Rate Control, en Type
- Hacé un click en el botón Service Management

System Summary	Bandwidth M	lanagement			
> DHCP	The Maximum Ba	ndwidth Provided by ISP			
System Management Dual WAN Bandwidth Management SNMP	Interface WAN1 WAN2	Upstream (Kbit/sec) 10240 10240	Downstrea 10240 10240	m (Kbil/sec)	
Discovery-Bonjour Diagnostic Factory Default Firmware Upgrade Restart	Bandwidth Manag	jement Type	Priority		
Backup and Restore Port Management Firewall Cisco ProtectLink Web VPN Log Wizard	Interface : Service : Direction : Priority : Enable :	WAN1 WAN2 DNS (UDP/53-53) Service Management Upstream • High •	•		

 Aquí definií el nombre del servicio, protocolo y rango de puertos (este proceso es similar al visto en Redirección de Puertos). Agregá los siguientes parámetros usando el botón Add to List

0	Service Name: SIP	Protocol: UDP
0	Service Name: RTP	Protocol: UDP
0	Service Name: RTP2	Protocol: UDP

Service Managem	nent - Mozilla Firefox	X
http://200.69.25	3.233:8080/service02.htm	☆
Service Name : Protocol : Port Range :	SIP UDP - 17 5060 to 5090	
-	Add to list	
DNS [UDP/53-53] FTP [TCP/21-21] HTTP secondary [TC] HTTPS [TCP/443-44] HTTPS Secondary [TC] TFTP [UDP/69-69] IMAP [TCP/143-143] NNTP [TCP/143-143] SNMP [TCP/149-110] SNMP [TCP/157-15]	P/8080~8080] 3] CP/8443~8443]]]]	H
	Delete Add New	
OK Cance	el Close	
Listo		

Port Range: 5060 to 5090 Port Range: 16000 to 18000 Port Range: 40000 to 42000

🥹 Service Management - Mozilla Firefox	
http://200.69.253.233:8080/service02.htm	☆
Service Name : SIP	
Protocol : UDP 🔻 17	
Port Range : 5060 to 5090	
Update	
[L2TP [UDP/1701-1701] PPTF [CVP/1723-1723] [P3ec [UDP/500-500] ESP [ESP/0-0] GRE [GRE0-0] All IP Traffic [ALL/0-0] RDP [CVP/389-3389] Senidor [ICP/9876-9876] Backup [CVP/432-5432] EJCPUDP/2000-5000] RTP [UDP/16000-18000] RTP2[UDP/2000-5000]	
Delete Add New	
OK Cancel Close	
Listo	

Hacé un click en el botón OK para continuar



- Sobre los servicios definidos anteriormente (SIP, RTP y RTP2) especificá los siguientes parámetros:
 - Elegí la interfaz sobre la cual se aplica la priorización en Interface. En este caso será WAN1
 - Elegí el servicio en el combo-box Service. En el ejemplo se muestra para SIP
 - Elegí la dirección del tráfico a priorizar en **Direction**. En la imagen se ve **Upstream**, es decir subida.
 - Elegí prioridad alta usando el valor High en Priority
 - Tildá la opción Enable
- Este procedimiento debe repetirse de forma tal que cada servicio se monitoree tanto en **Upstream** como en **Downstream**, quedando 2 renglones en la lista por cada uno de ellos.

System Summary	
	Bandwidth Management Type
Setup	
	Type : ORate Control OPriority
 System Management Dual WAN Bandwidth Management 	Interface : WAN1 WAN2 Service : SIP (UDP/5060-5090)
SNMP	
Discovery-Bonjour Discoverie	Service Management
Eactory Default	Direction : Upstream -
Firmware Upgrade	
Restart	
Backup and Restore	Enable :
Port Management	Add to list
Firewall	
Cisco ProtectLink Web	SIP(UDP/5060~5090)(Upstream)=>High=>WAN1
VPN	RTP[UDP/16000~18000](Upstream)=>High=>WAN1
▶ Log	RTP2[UDP/40000~42000](Downstream)=>High=>WAN1
Wizard	RTP2[UDP/40000~42000](Upstream)=>High=>WAN1
	Delete Add New
	View Save Cancel
System Summary	
Setup	Bandwidth Management Type
DHCP	
 System Management 	Type: O Rate Control O Priority
D	
Dual WAN	
Bandwidth Management	Interface : WAN1 WAN2
Bandwidth Management SNMP Discover-Boniour	Interface : WAN1 WAN2 Service : SIP [UDP/5060-5090]
Duai WAN Bandwidth Management SNMP Discovery-Bonjour Diagnostic	Interface : WAN1 WAN2 Service : SIP (UDP/5060-5090) - Service Management
Dial WAN Bandwidh Management SNMP Discovery-Bonjour Diagnostic Factory Default	Interface : VAN1 WAN2 Service : SIP (UDP/5060-5090) · Service Management
Duai wAN Bandwidth Management SNMP Discovery-Bonjour Diagnostic Factory Default Firmware Upgrade	Interface : VWAN1 WWAN2 Service : SIP (UDP/5060-5090) Service Management Direction : Upstream
Duai wAN Bandwidth Management SNMP Discovery-Bonjour Disgnostic Factory Default Firmware Upgrade Restart	Interface : VWAN1 WAN2 Service : SIP (UDP/5060-5090) Service Management Direction : Upstream Priority : High
Dual www Bandwidth Management SNIMP Discoveny-Bonjour Diagnostic Factory Default Firmware Upgrade Restart Backup and Restore	Interface : WAN1 WAN2 Service : SIP [UDP/5060-5090] • Service Management Direction : Upstream • Priority : High • Enable : V
Udai YAAN Bandwidhi Management SNMP Discovery-Bonjour Diagnostic Factory Default Firmware Upgrade Restart Backup and Restore > Port Management	Interface : WAN1 WAN2 Service : SIP [UDP/5060-5090] Service Management Direction : Upstream Priority : High Enable :
Dual wAN BandWidh Management SNMP Discover,-Bonjour Diagnostic Factory Default Firmware Upgrade Restart Backup and Restore > Port Management > Firewall	Interface : V WAN1 WAN2 Service : SIP (UDP/5060-5090) Service Management Direction : Upstream Priority : High Enable : V Update
Uuai www Bandwidh Management SNMP Discovery-Bonjour Diagnostic Fadory Default Firmware Upgrade Restart Backup and Restore > Port Management > Firewall > Cisco ProtectLink Web	Interface : WAN1 WAN2 Service : SIP (UDP/5060-5090) Service Management Direction : Upstream Priority : High Enable : Update SIP[UDP/5060-5090](Upstream)=>High=>WAN1
Uual WAN BandWidth Menagement SNMP Discoveny-Bonjour Diagnostic Factory Default Firmware Upgrade Restart Backup and Restore > Port Management > Firewall > Cisco ProtectLink Web > VPN	Interface : WAN1 WAN2 Service : SIF [UDP/5060-5090] Service Management Direction : Upstream Priority : High Enable : Update SIF[UDP/5060-5090](Upstream)=>High=>WAN1 SIF[UDP/5060-5090](Upstream)=>High=>WAN1 SIF[UDP/5060-5090](Upstream)=>High=>WAN1
Uual WAN Bandwidh Management SNMP Discorey-Bonjour Diagnostic Factory Default Factory Default Factory Default Factory Default Restart Backup and Restore A claus And Restore Factory ProtectLink Web VPN Log	Interface : WAN1 WAN2 Service : SIP [UDP/5060-5090] Service Management Direction : Upstream Priority : High Finable : Update SIP[UDP/5060-5090]Ubstream]==High==WAN1 SIP[UDP/5060-5090]Ubstream]==High==WAN1 RTPULDP/10000-15000[Upstream]==High==WAN1 RTPULDP/10000-15000[Upstream]==High==WAN1 RTPULDP/10000-15000[Upstream]==High==WAN1
Uual WAN Bandwidh Management SNMP Discovery-Bonjour Diagnostic Factory Default Fartware Upgrade Restart Backup and Restore > Port Management > Firewall > Cisco ProtectLink Web > VPN > Log Witzard	Interface : WAN1 WAN2 Service : SIP [UDP/5060-5090] Service Management Direction : Upstream Priority : High Finable : Update SIP[UDP/5060-5090](Upstream)=High=>WAN1 RTP[UDP/5060-5090](Upstream)=High=>WAN1 RTP[UDP/5060-5090](Upstream)=High=>WAN1 RTP[UDP/5060-5090](Upstream)=High=>WAN1 RTP[UDP/5060-5090](Upstream)=High=>WAN1 RTP[UDP/5060-5090](Upstream)=High=>WAN1 RTP[UDP/5000-5090](Upstream)=
Uual WAN Bandwidh Management SNMP Discover,-Bonjour Diagnostic Factory Default Firmware Upgrade Restart Backup and Restore > Port Management > Firewall > Cisco ProtectLink Web > VPN > Log Wizard	Interface : WAN1 WAN2 Service : SIP [UDP/5060-5090] Service Management Direction : Upstream Priority : High Enable : U SIP[UDP/5060-5090](Destream)=>High=>WAN1 RTPUL0P/16000-18000[Upstream)=>High=>WAN1 RTPUL0P/16000-18000[Upstream)=>High=>WAN1 RTP2UDP/16000-18000[Upstream)=>High=>WAN1 RTP2UDP/16000-18000[Upstream)=>High=>WAN1 RTP2UDP/16000-18000[Upstream)=>High=>WAN1 RTP2UDP/16000-18000[Upstream)=>High=>WAN1
Uual WAN BandWidh Management SNMP Discover, Bonjour Diagnostic Factory Default Firmware Upgrade Restart Backup and Restore > Port Management > Firewall > Cisco ProtectLink Web > VPN > Log Wizard	Interface : W WAN1 WAN2 Service : SIP [UDP/5060-5090] Service Management Direction : Upstream Phonty : High Enable : Update SIP[UDP/5060-5090](Upstream)=>High=>WAN1 RTPULDP/6060-5090[(Upstream)=>High=>WAN1 RTPULDP/6000-43000[(Upstream)=>High=>WAN1 RTPULDP/6000-43000[(Upstream)=>High=>WAN1 RTPULDP/6000-43000[(Upstream)=>High=>WAN1 RTPULDP/6000-43000[Upstream)=>High=>WAN1 RTPULDP/6000-43000[Upstream)=>High=>WAN1 RTPULDP/6000-43000[Upstream)=>High=>WAN1
Uual WAN SendWidth Meagement SNMP Discovery-Bonjour Diagnostic Factory Default Firmware Upgrade Restart Backup and Restore > Port Management > Firewalt > Cisco ProtectLink Web > VPN > Log Wizard	Interface : WAN1 WAN2 Service : SIF [UDP/5060-5090] • <u>Service Management</u> Direction : Upstream • Priority : High • Enable : <u>Update</u> SIF[UDP/5060-5090](Upstream)=>High=>WAN1 SIF[UDP/5060-5090](Upstream)=>High=>WAN1 RTP[UDP/5000-5090](Upstream)=>High=>WAN1 RTP[UDP/5000-5090](Upstream)=>High=>WAN1 RTP[UDP/5000-5090](Upstream)=>High=>WAN1 RTP[UDP/5000-5090](Upstream)=>High=>WAN1 RTP[UDP/5000-5090](Upstream)=>High=>WAN1 RTP[UDP/5000-5090](Upstream)=>High=>WAN1
Uual WAN Sandwidh Management SNMP Discorey-Bonjour Diagnostic Factory Default Factory Default Factory Default Restart Backup and Restore Packup and Restore Restart Backup and Restore Packup and Restore Firewall Cisco ProtectLink Web VPN Log Wizard	Interface : WAN1 WAN2 Service : SIP [UDP/6060-5090] • Service Management • • Direction : Upstream • Priority : High • • Enable : • • SIPUDP/6060-5090[Upstream]=+High=>WAN1 • SIPUDP/6060-5090[Upstream]=+High=>WAN1 • RTPUDP/6060-5090[Upstream]=+High=>WAN1 • RTPUDP/6060-5090[Upstream]=+High=>WAN1 • RTPUDP/6060-4000[Upstream]=+High=>WAN1 • RTPUDP/6000-4000[Upstream]=+High=>WAN1 •
Dual wAN Bandwidh Management SNMP Discovery-Bonjour Diagnostic Factory Default Fartware Upgrade Restart Backup and Restore > Port Management > Firewall > Cisco ProtectLink Web > VPN > Log Wizard	Interface : WAN1 WAN2 Service : SIP [UDP/5060-5090] Service Management Direction : Upstream Priority : High Enable : Update SIP[UDP/5060-5090](Upstream)==+Hgh==>WA11 RTPULDP/5060-5090](Upstream)==+Hgh==>WA11 RTPULDP/5000-5090](Upstream)==+Hgh==>WA11 RTPULDP/5000-5090](Downsteam)==+Hgh==>WA11 RTPULDP/5000-5090](Downsteam)==+Hgh==>WA11 RTP2UDP/5000-5090](Downsteam)==+Hgh==>WA11 RTP2UDP/40000-42000](Downsteam)==+Hgh==>WA11
Dual wAN Bandwidh Management SNMP Discover,-Bonjour Diagnostic Factory Default Factory Default Fartware Upgrade Restart Backup and Restore > Port Management > Firewall > Cisco ProtectLink Web > VPN > Log Wizard	Interface : WAN1 WAN2 Service : SIP [UDP/5060-5090] Service Management Direction : Upstream Priority : High Enable : Update SIP[UDP/5060-5090]Upstream]=+High=>WAN1 RTP[UDP/5060-5090]Upstream]=+High=>WAN1 RTP[UDP/5060-5090]Upstream]=+High=>WAN1 RTP[UDP/5060-5090]Upstream]=+High=>WAN1 RTP2[UDP/6000-42000](Downstream)=+High=>WAN1 RTP2[UDP/40

Con esto habremos finalizado la Configuración Básica y Avanzada del Router.

Para conocer más sobre el servicio de **Internet**, te recomendamos la lectura de los instructivos publicados en el **Centro de Ayuda IPLAN** en <u>http://clientes.iplan.com.ar/centrodeayuda</u>

Esperamos que el presente instructivo te haya sido de utilidad.

Centro de Atención Técnica - IPLAN