

Competencia Disciplinar: Configura el equipo requerido que permite la operación de una red de cobertura local que satisface las necesidades de organizaciones pequeñas identificando diferentes opciones de infraestructura tecnológica

Los espacios de coworking o espacios de trabajo colaborativo son instalaciones de trabajo que varias personas comparten con el fin de mejorar su productividad, hacer networking e inclusive reducir los costos de servicios y renta de un espacio físico.

El coworking se ha vuelto una gran oportunidad de negocio en México y otros países ya que representa una opción favorable para pequeñas empresas, startups y freelancers ^[1]. Un ejemplo de estos negocios es **COHAUS**, un espacio de coworking que ofrece desde espacios libres de trabajo y escritorios fijos, hasta salas de juntas y oficinas bien equipadas. ^[2]

Vamos a considerar el equipo de red de un negocio de coworking. Cada pieza de infraestructura pertenece al segmento de **administradores** o al segmento de **usuarios**. El primer segmento está dedicado al personal del establecimiento y está constituido de no más de 18 equipos terminales. Entre estos equipos están: un servidor local, un teléfono IP, una impresora, una cámara web, un punto de venta y una PC para el administrador (manager). Las direcciones IP de los equipos terminales se asignan de manera estática (manualmente).

Mientras tanto, en el segmento de **usuarios** simplemente se encuentran los equipos personales conectados físicamente a la red. En este segmento de red hay un máximo de 100 equipos a conectar. La asignación de direcciones IP a los equipos del segmento de usuarios se realiza por **DHCP**.

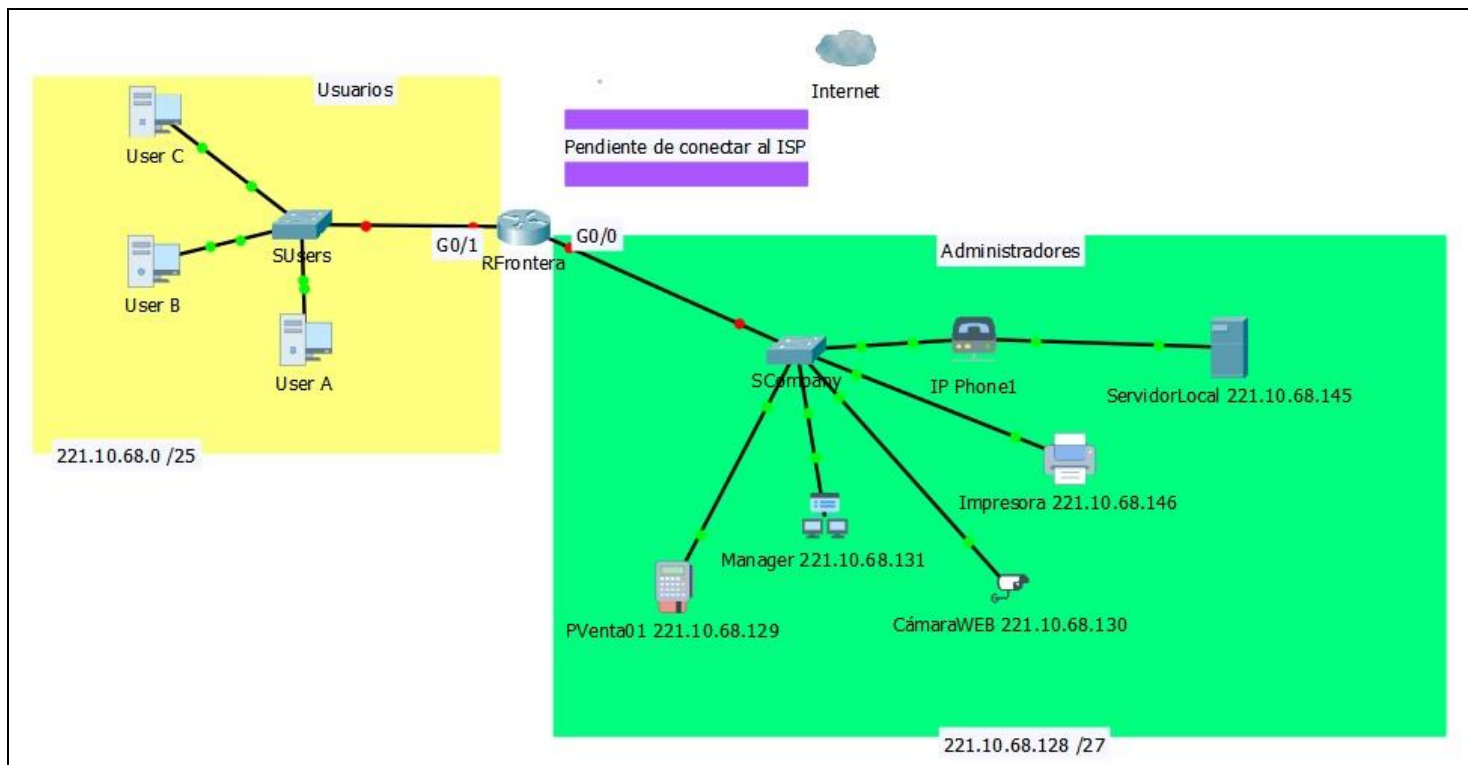
Ahora te queda como reto, diseñar y configurar los equipos de interconexión de la red usando el simulador de Packet Tracer.

Referencias

[1] Solís, A. (2018). *Guía Forbes de Coworking: todo lo que necesitas saber*. Recuperado de <https://www.forbes.com.mx/guia-forbes-de-coworking-todo-lo-que-necesitas-saber/>

[2] COHAUS. (s.f.). *Paquetes*. Recuperado de <https://cohaus.work/paquetes/>

Utiliza la aplicación del PacketTracer de CISCO y la gráfica incluida en este documento para realizar: (a) la configuración del router y switches (b) la instalación del servicio de DHCP para asignar direcciones a los equipos terminales del segmento usuarios, (c) las pruebas de conectividad necesarias y que permitan verificar la configuración correcta de los equipos de interconexión, de los equipos terminales y de los servicios de Telnet en el router y los switches.



Diseño físico de la red.

La dirección IP a utilizar para realizar la configuración de los equipos de interconexión y la configuración de cada equipo terminal, es **221.10.68.0** con prefijo original de red **/24**.

El **VLSM** calculado con base en la descripción de equipos terminales que se requieren conectar en cada segmento de red está indicado en la siguiente tabla.

Requisitos de Conectividad	Prefijo o Red	IP Bloque	Máscara	Primera IP válida	Última IP válida
Usuarios 100 hosts	/25	221.10.68.0	255.255.255.128	221.10.68.1	221.10.68.126
Administradores 18 hosts	/27	221.10.68.128	255.255.255.224	221.10.68.129	221.10.68.158

- Asigna y escribe en cada línea de la tabla, las direcciones IP de las interfaces de los equipos de interconexión, su máscara en notación punto decimal y de conforme a lo que se indica en la siguiente tabla.

Device	Interface	IP Address	Subnet Mask	Default Gateway
RFrontera	G0/0	Última IP válida de la subred		N/A
	G0/1	Última IP válida de la subred		N/A
	Lo0	1.1.1.1	255.255.255.224	N/A
SUsers	VLAN 1	Penúltima IP válida de la subred		
SCompany	VLAN 1	Penúltima IP válida de la subred		
User A	NIC	Asignada por DHCP	Asignada por DHCP	Asignada por DHCP
User B	NIC	Asignada por DHCP	Asignada por DHCP	Asignada por DHCP
User C	NIC	Asignada por DHCP	Asignada por DHCP	Asignada por DHCP
PVenta01	NIC	221.10.68.129	255.255.255.224	221.10.68.158
CámaraWEB	NIC	221.10.68.130	255.255.255.224	221.10.68.158
Manager	NIC	221.10.68.131	255.255.255.224	221.10.68.158
ServidorLocal	NIC	221.10.68.145	255.255.255.224	221.10.68.158
Impresora	NIC	221.10.68.146	255.255.255.224	221.10.68.158

- b. Realiza la configuración de las interfaces del **Router Frontera**. Deshabilitar el **DNS**. Asignar password **cisco** al Line Console 0. Asignar **class** como password del enable. Hostame **RFrontera**. Configurar un **banner** de prevención de acceso al router. Asignar **cisco** al password de la Line Vty 0 4.
- c. Realiza la configuración del switch **SUsers**. Deshabilitar el **DNS**. Asignar password **cisco** al Line Console 0. Asignar **class** como password del enable. Hostame **SUsers**. Configurar un **banner** de prevención de acceso al router. Asignar cisco al password de la Line Vty 0 15. Configurar la **VLAN1** con los datos de la tabla y el **default Gateway** de este switch.
- d. Realiza la configuración del switch **SCompany**. Deshabilitar el **DNS**. Asignar password **cisco** al Line Console 0. Asignar **class** como password del enable. Hostame **SCompany**. Configurar un **banner** de prevención de acceso al router. Asignar cisco al password de la Line Vty 0 15. Configurar la **VLAN1** con los datos de la tabla y el **default Gateway** de este switch.

- e. Utiliza la información de la tabla y configura manualmente la dirección IP, máscara y puerta de enlace predeterminada para cada equipo terminal del segmento de **administradores**.

Para comprobar la configuración realizada, ejecuta un **ping** desde los equipos terminales **User A** y **User C** del diseño de red, a la dirección IP de la interfaz **LoopBack 0** del router frontera. Si el **ping** es exitoso, tu configuración en ese segmento de red está correcta. En caso contrario, deberás encontrar y corregir la falla.

Desde la **User A** y **User B** utiliza la aplicación **Telnet** y accede a la dirección IP del **switch SUsers** y **SAdministradores**. Utiliza password **cisco** y **class** para acceder a modo de configuración del switch. Si el **Telnet** es exitoso, la configuración está correcta. En caso contrario, deberás encontrar y corregir la falla.

Desde **User C** utiliza el navegador **web** de la terminal y utilizando la dirección IP del server **accede** al **ServidorLocal** y utiliza la IP de la cámara para acceder, con el navegador web de la terminal, al servidor **CámaraWEB**. Si el acceso a los servidores es exitoso, tu configuración es correcta. En caso contrario, deberás encontrar y corregir la falla.

Agrega imágenes (impresión de pantalla) de las pruebas de conectividad realizadas.



