Interconexión de Redes TC2022

Caso Espacio de Coworking

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, o simplemente ahorrar en costos de servicios y renta.

Caso Espacio de Coworking

El coworking se ha vuelto una gran industria 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 en la ciudad de Querétaro que ofrece desde espacios libres de trabajo y escritorios fijos, hasta salas de juntas y oficinas bien equipadas. [2]

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/

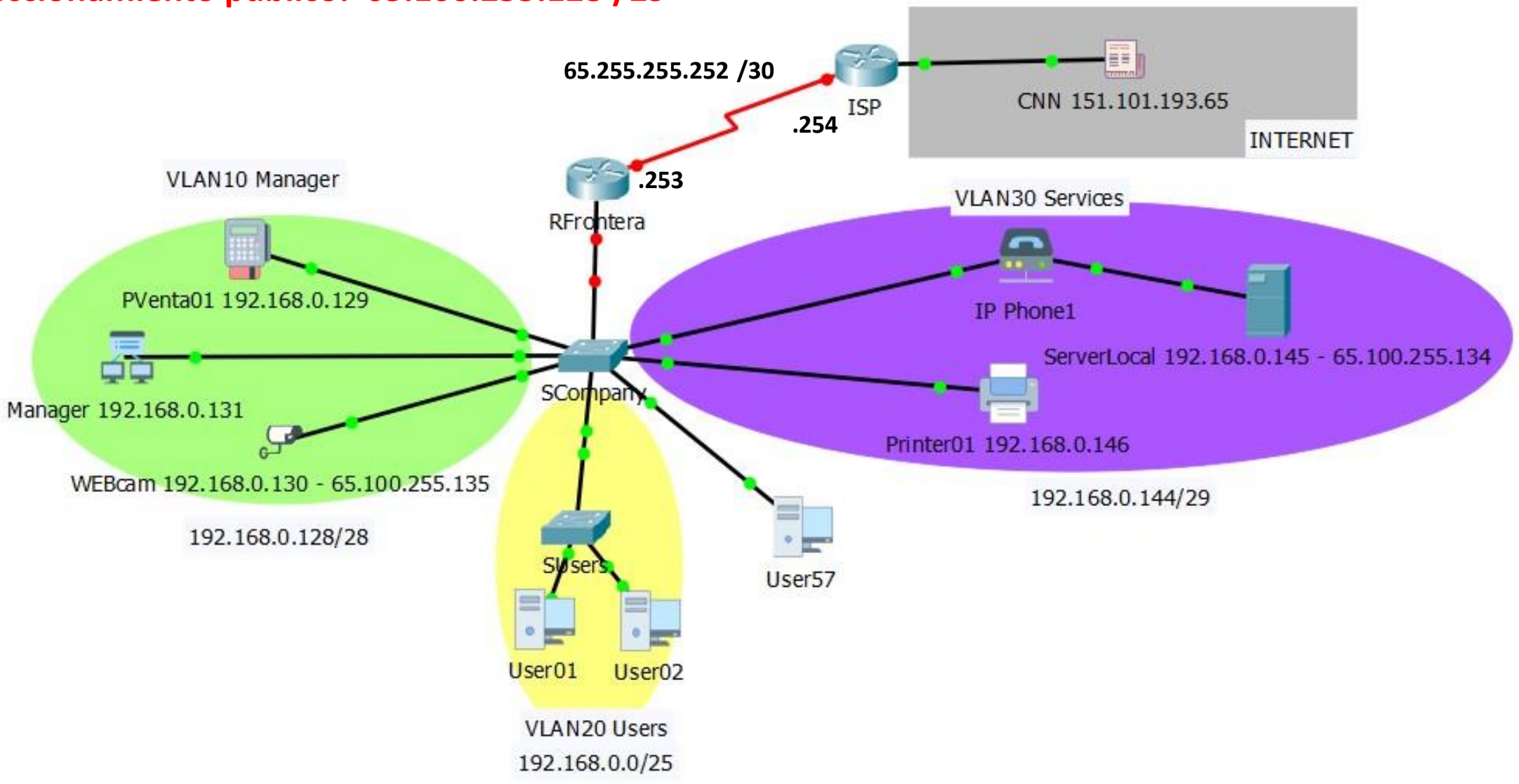
[2] COHAUS. (s.f.). *Paquetes*. Recuperado de https://cohaus.work/paquetes/

Caso Espacio de Coworking

Nuestro reto el día de hoy es trabajar con un diseño físico de red en **Packet Tracer** y realizar la programación de los equipos de interconexión y la instalación de los servicios de **DHCP** y **NAT** para lograr la conectividad de un espacio de coworking con la red Internet.

Caso Espacio de Coworking

Direccionamiento público: 65.100.255.128 /29



Restricciones y consideraciones del cliente

Debemos realizar el diseño con base en restricciones que han sido establecidas por el cliente.

1. Debemos utilizar **VLSM**.
2. La **IP pública** para conectarnos al **ISP** es **65.255.255.253/30**
3. Debemos utilizar tres **VLANS** (Manager, Users, Services)
4. Solo el grupo de **Users** obtiene dirección IP dinámica (**DHCP**)
5. Debemos conectar la red local a los servicios de Internet, por lo que utilizaremos el siguiente bloque de IPs públicas **65.100.255.128 / 29**
6. Por lo limitado de las IPs públicas debemos utilizar **PAT (NAT overload)**.
7. Servidor y Cámara WEB tienen **NAT estático**. Las IP públicas para estos servicios ya han sido seleccionadas.
8. Realizar las pruebas de conectividad necesarias.

Tipos de NAT

Hay 4 formas de instalar el servicio de NAT:

1. **NAT estático.** Se traduce una dirección IP privada por una dirección IP pública.

NAT dinámico:

2. **NAT puro:** Por cada dirección IP privada se traduce a una dirección IP pública, lo cual consume muchas direcciones IPs públicas.
3. **NAT con sobrecarga (PAT):** Muchas direcciones IP privadas se traducen con pocas direcciones IP públicas. Se utiliza la combinación de direccionamiento **IP capa 3** y el **puerto capa 4**.
4. **Port forwarding:** Muchas direcciones IP privadas se traducen con una dirección IP pública, incluyendo direcciones estáticas como los servidores, impresoras, etc.

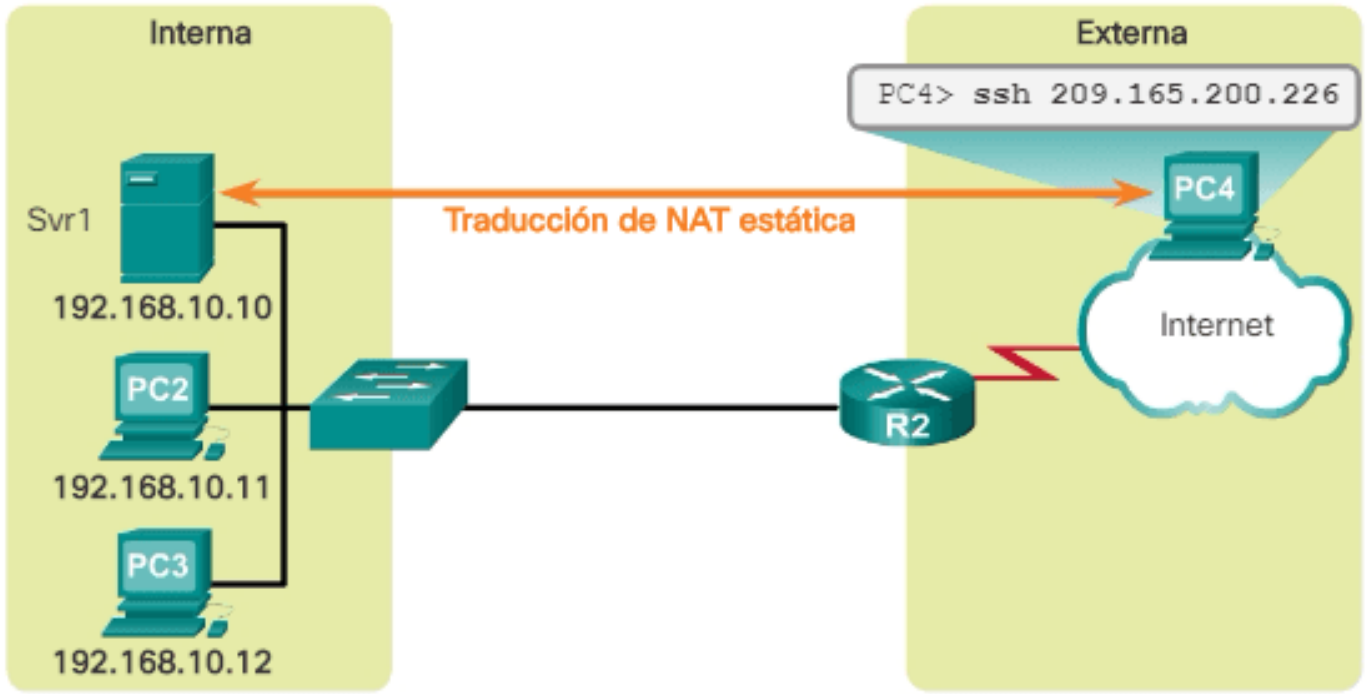
NAT estático

Se traduce una dirección IP privada por una dirección IP pública.

En este ejemplo, el **R2** se configuró con las asignaciones estáticas para las direcciones locales internas del **Svr1**, la **PC2** y la **PC3**. Cuando estos dispositivos envían tráfico a Internet, sus direcciones locales internas se traducen a las direcciones globales internas configuradas. Para las redes externas, estos dispositivos tienen direcciones IPv4 públicas.

Tabla de NAT estática

Dirección local interna	Dirección global interna: direcciones a las que se puede llegar a través del R2
192.168.10.10	209.165.200.226
192.168.10.11	209.165.200.227
192.168.10.12	209.165.200.228



NAT dinámico

Por cada dirección IP privada se traduce dinámicamente a una dirección IP pública.

Utiliza un conjunto de direcciones públicas y las asigna según el orden de llegada. Cuando un dispositivo interno solicita acceso a una red externa, se asigna una dirección IPv4 pública disponible del conjunto.

En el ejemplo, la **PC3** accede a Internet mediante la primera dirección disponible del conjunto de NAT dinámico. Las demás direcciones siguen disponibles para utilizarlas.

Conjunto de NAT para IPv4

Dirección local interna	Conjunto de direcciones globales internas: direcciones a las que se puede llegar a través del R2
192.168.10.12	209.165.200.226
Disponibles	209.165.200.227
Disponibles	209.165.200.228
Disponibles	209.165.200.229
Disponibles	209.165.200.230

NAT con sobrecarga (PAT)

Muchas direcciones IP privadas se traducen con pocas direcciones IP públicas. Se utiliza la combinación de direccionamiento **IP capa 3** y el **puerto capa 4**.

Cuando un dispositivo inicia una sesión TCP/IP, genera un valor de puerto de origen TCP o UDP para identificar la sesión de forma exclusiva. Cuando el router NAT recibe un paquete del cliente, utiliza su número de puerto de origen para identificar de forma exclusiva la traducción NAT específica.

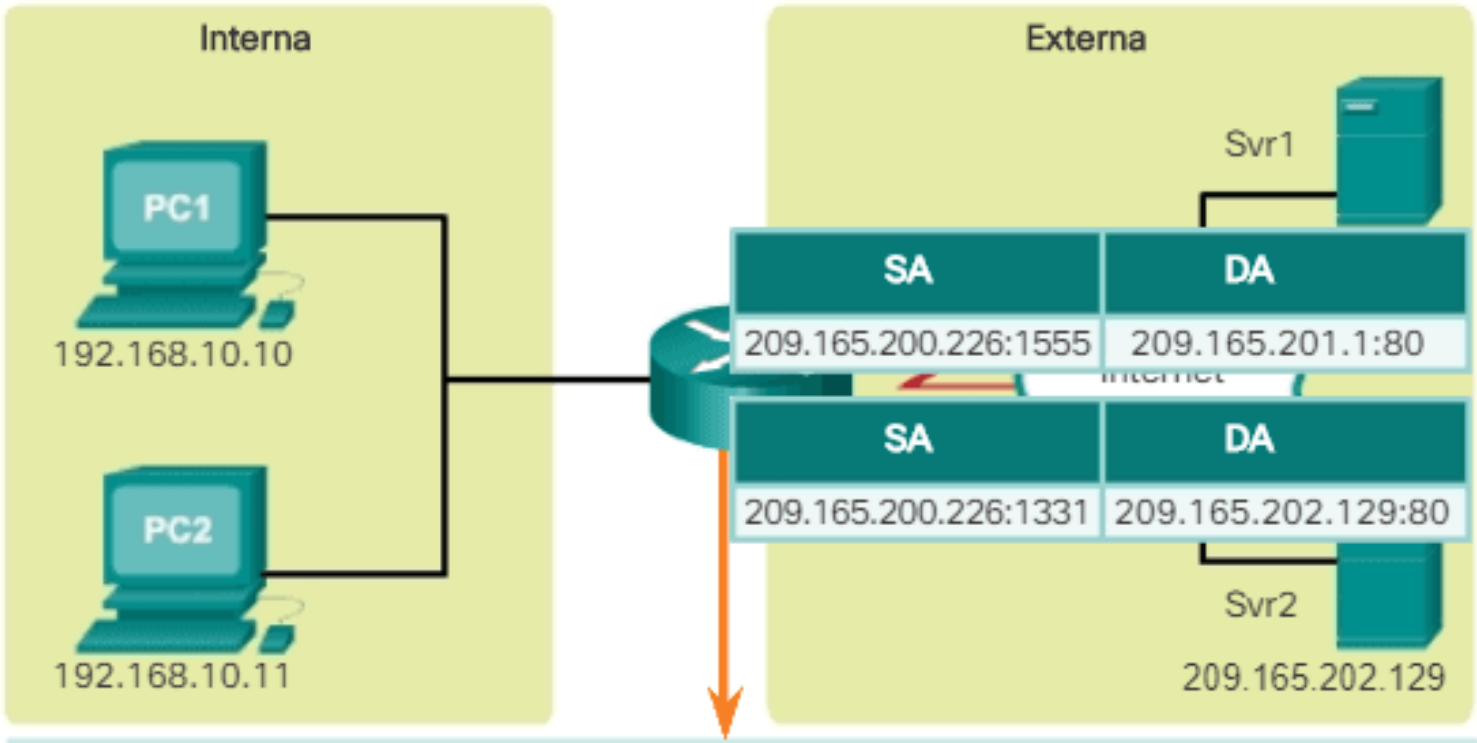


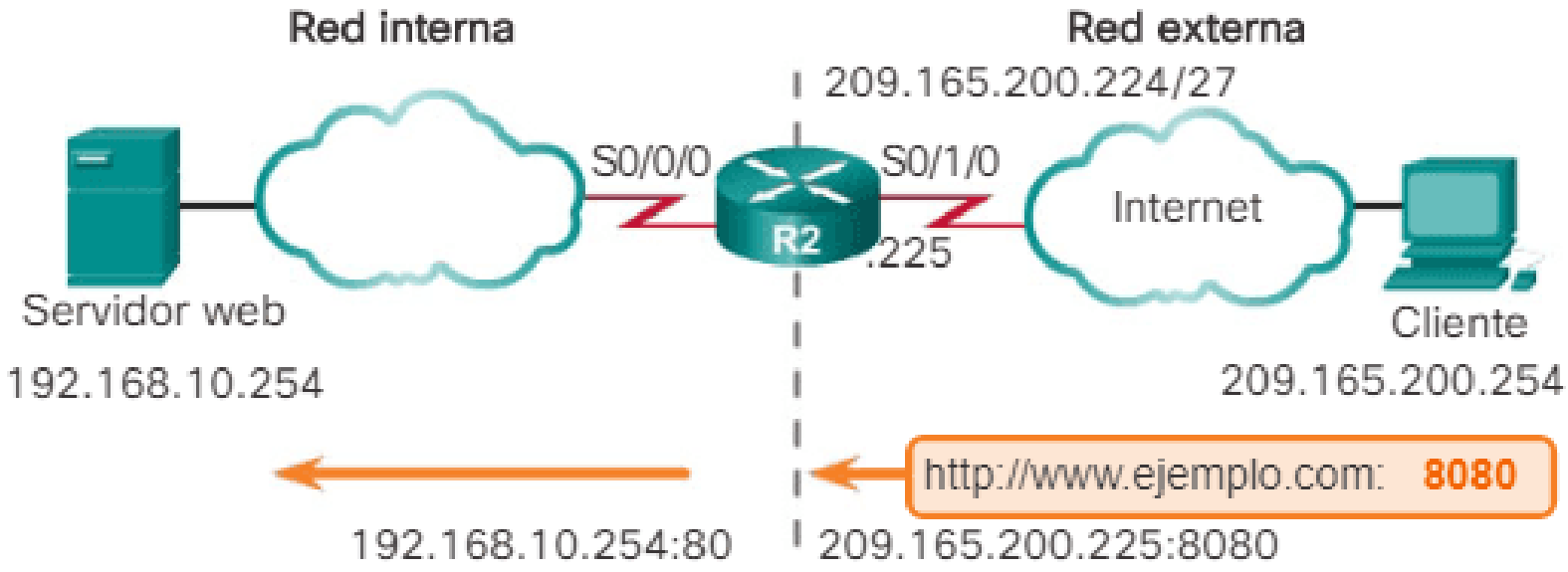
Tabla NAT con sobrecarga

Dirección IP global interna	Dirección IP local interna	Dirección IP local externa	Dirección IP global externa
209.165.200.226:1555	192.168.10.10:1555	209.165.201.1:80	209.165.201.1:80
209.165.200.226:1331	192.168.10.10:1331	209.165.202.129:80	209.165.202.129:80

Port forwarding

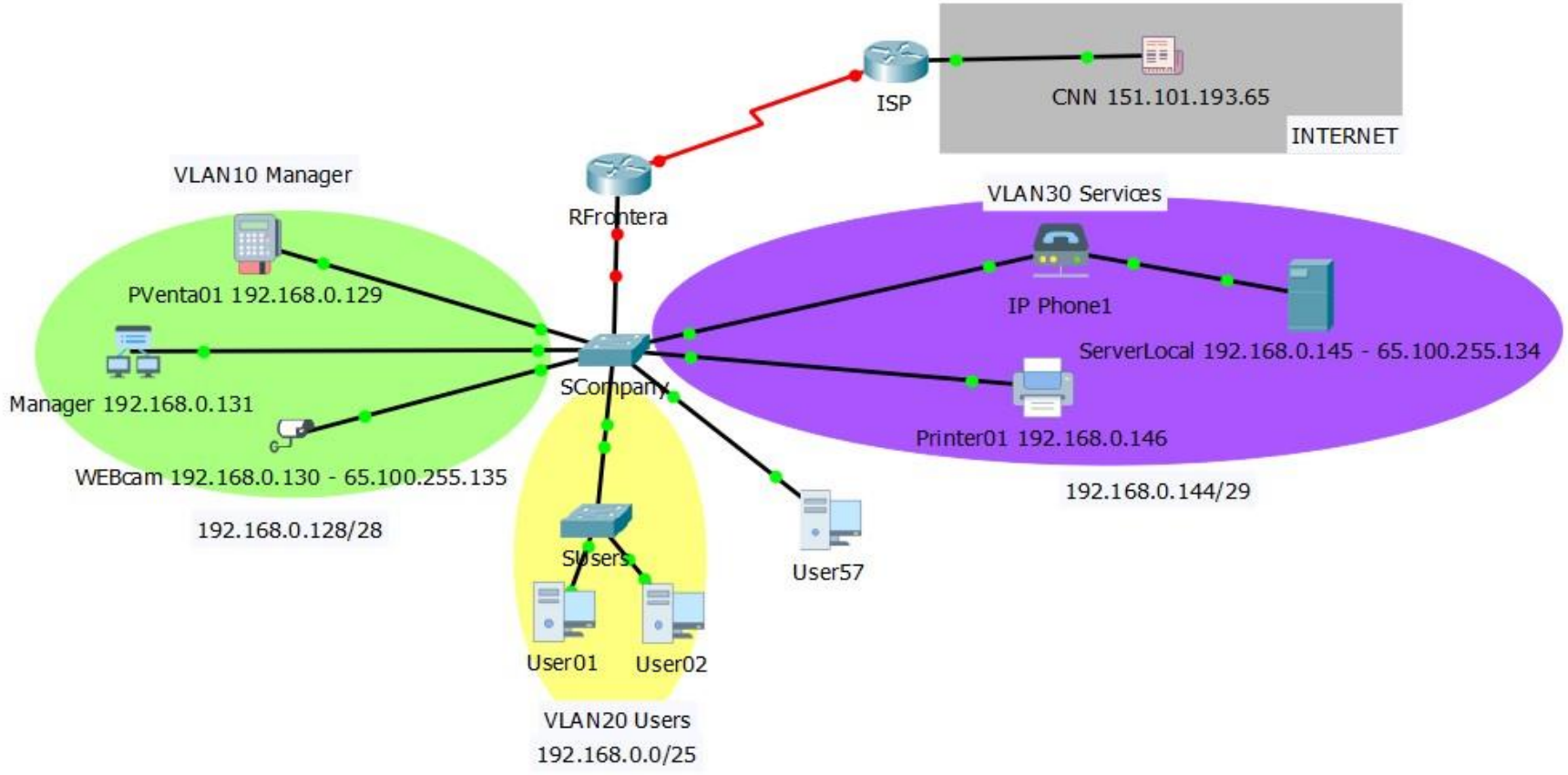
Muchas direcciones IP privadas se traducen con una dirección IP pública, incluyendo direcciones estáticas como los servidores, impresoras, etc.

Para poder instalar **port forwarding** necesito realizar **una traducción estática, una dirección IP privada, una dirección IP pública,** el **protocolo** (tcp o udp)**,** el **puerto** por el que vamos a **escuchar** y el **puerto por el que me van a contactar desde el exterior.**



Configuración del servicio de DHCP

1. Tenemos tres subredes asociadas con las **VLANs 10, 20 y 30**.
2. La subred de los usuarios (VLAN 20) es a la única a la que se le asignarán direcciones IP dinámicas.
3. Configurar primero las excepciones.
4. Configurar DHCP en el **RFrontera** como un servicio **centralizado**.



Configuración mínima de un servicio DHCP

1. Excluir las direcciones estáticas del pool de DHCP.

   ip dhcp excluded-address Dir_IP_Inicial Dir_IP_Final

2. Definir un **pool de direcciones dinámicas** que serán asignadas cuando sean solicitadas.

   ip dhcp pool NombrePool

   network dirIP_inicial Máscara de subred

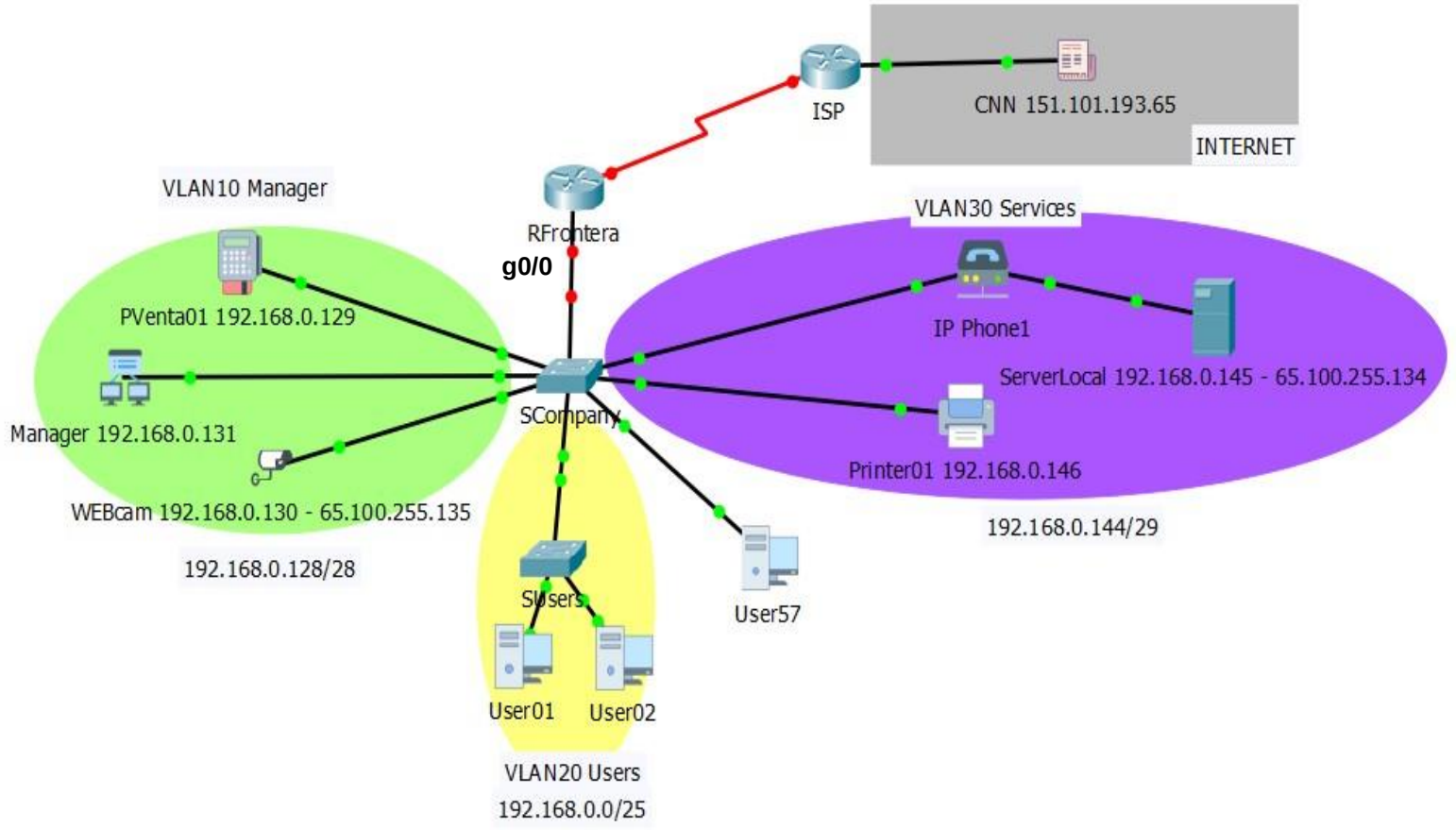
3. Establecer la puerta de enlace predeterminada (default Gateway):

   default-router dirIP

Configuración de las VLANs

Las **VLANs** son redes virtuales que permiten **segmentar el tráfico** y tener distintos dominios de broadcast en una misma interface del router, con el uso de las subinterfaces.

- El definir subinterfaces en el **RFrontera** implica que la interface **g0/0** recibe peticiones de la **vlan 10** , **vlan 20** y **vlan 30**.
- Las subinterfaces se definen con la interface **g0/0** y se le concatena la **subinteface asociada** con la vlan **g0/0.10**.
- El protocolo de encapsulamiento debe incluir el **id** de la **vlan**.
- La **dirección IP de la subinterface** va a ser la **última dirección IP válida** de la subred o bloque.



Configuración de las VLANs

Comandos para el Router

! Sección para crear las subinterfaces asociadas a cada VLAN

int g0/0.VID

encapsulation dot1q VID

ip add DirIP Msk

! Hay que levantar todas las subinterfaces (lógicas). Si levanto la interfaz física se levantan todas las subinterfaces.

int g0/0

no shut

NOTAS:

- Todas las interfaces y subinterfaces de la red se configurarán como **ip nat inside**, ya que es una traducción interna.
- La única interface **outside**, es la que se conecta con el ISP, ya que es la que se encargará de la traducción del direccionamiento privado a público.

Configuración de las VLANs

Pasos para configurar las **VLANs** en el **switch**:

1. Crear la **base de datos** de las **VLANs**
2. Asignar los **puertos de acceso** del switch a la VLAN correspondiente.
3. Definir el **puerto troncal** (puerto por el que va a salir el tráfico de las distintas VLANs).

Los puertos del switch han sido divididos de la siguiente forma:

- **F0/1-6** **VLAN 10 Management**
- **F0/7-19** **VLAN 20 Users**
- **F0/20-24** **VLAN 30 Services**

vlan 1 que es la **nativa**, está creada siempre por default.

Configuración de las VLANs

Comandos para el Switch

! Creación de las VLANs con nombre.

vlan VID

name NombreVLAN-asociadaVID

exit

! Asignación de los puertos de acceso a cada VLAN VID

interface Nombre_Interfaz

switchport mode access

switchport access vlan VID

! Definición del puerto troncal

interface Nombre_Interfaz

switchport mode trunk

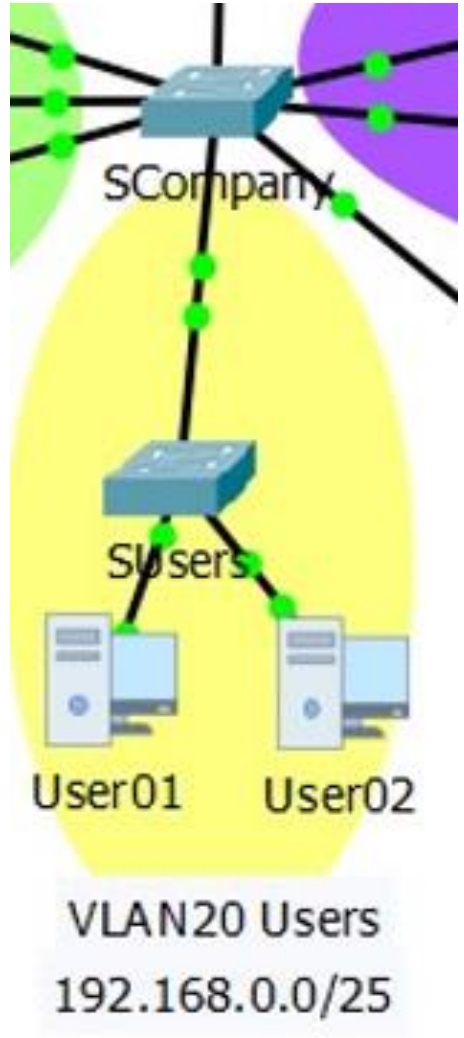
no shut

Configuración de las VLANs

Configurar el switch **SUsers**, que solamente ha sido puesto como una extensión del switch **SCompany**.

F0/7-19 **VLAN 20 Users**

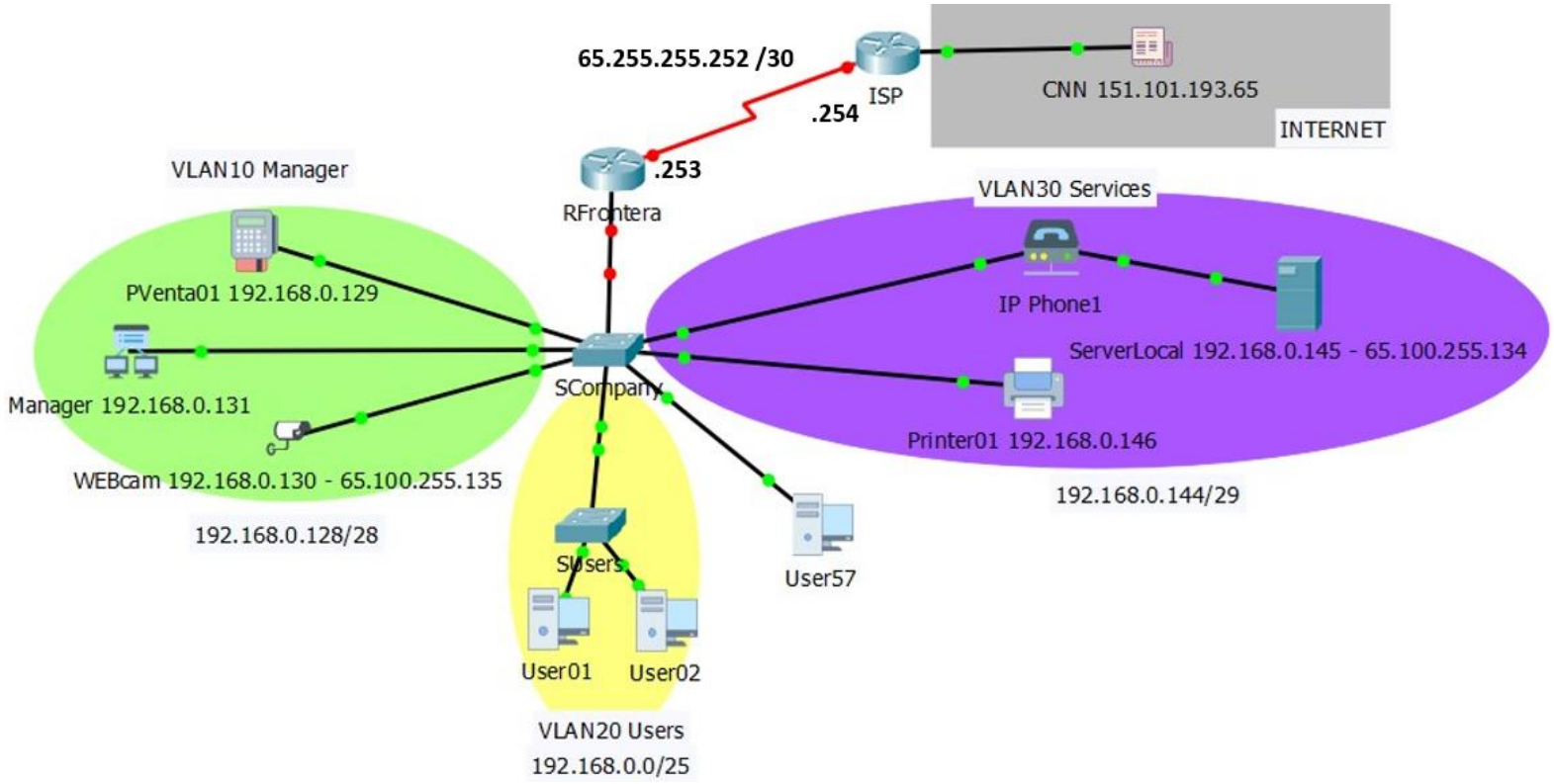
SUsers es una extensión de la **VLAN 20** y todos los puertos de este switch pertenecen a esta VLAN.



Configuración de rutas por default

1. Configurar la IP de la interface **s0/0/0** del **RFrontera**.
2. No se requiere configurar un protocolo de ruteo, el ruteador **RFrontera** está configurado para trabajar como **router on stick** (una sola interfaz física se encarga de enrutar los paquetes de varias VLANs). Solamente debemos saber cómo el tráfico interno va a salir al exterior.
3. Establecer una **ruta por default** que se encargue de sacar el tráfico a Internet.

- Cuando definimos nuestra interface de salida (s0/0/0) tenemos una **ruta por default directamente conectada**
- Si utilizamos la dirección IP del siguiente router, tenemos una **ruta por default recursiva.**
- Si concatenamos la interface de salida de nuestro router y la IP del siguiente router, tenemos una **ruta por default completamente conectada.**



Configuración de NAT

1. Definir un **pool de direcciones globales (públicas)** que serán asignadas cuando sean necesarias.

   ip nat pool Nombre dirIP-inicial dirIP-final netmask MáscaraSubneteo

2. Definir una **ACL estándar** (defino las direcciones IP privadas que tienen permiso a ser traducidas): :

   access-list Número permit dirIP-inicial WildMask_ACL

3. Establecer la **traducción dinámica de direcciones** utilizando la ACL definida.

   ip nat inside source { **list** {**Número | Nombre**} **pool NOMBRE [overload]** | **static** IP-local IP-Global }

4. Especificar las **interfaces interiores y exteriores** (definir la acción que se va a realizar en cada una de las interfaces cuando tengamos el servicio de NAT instalado)

   interface Tipo-Número

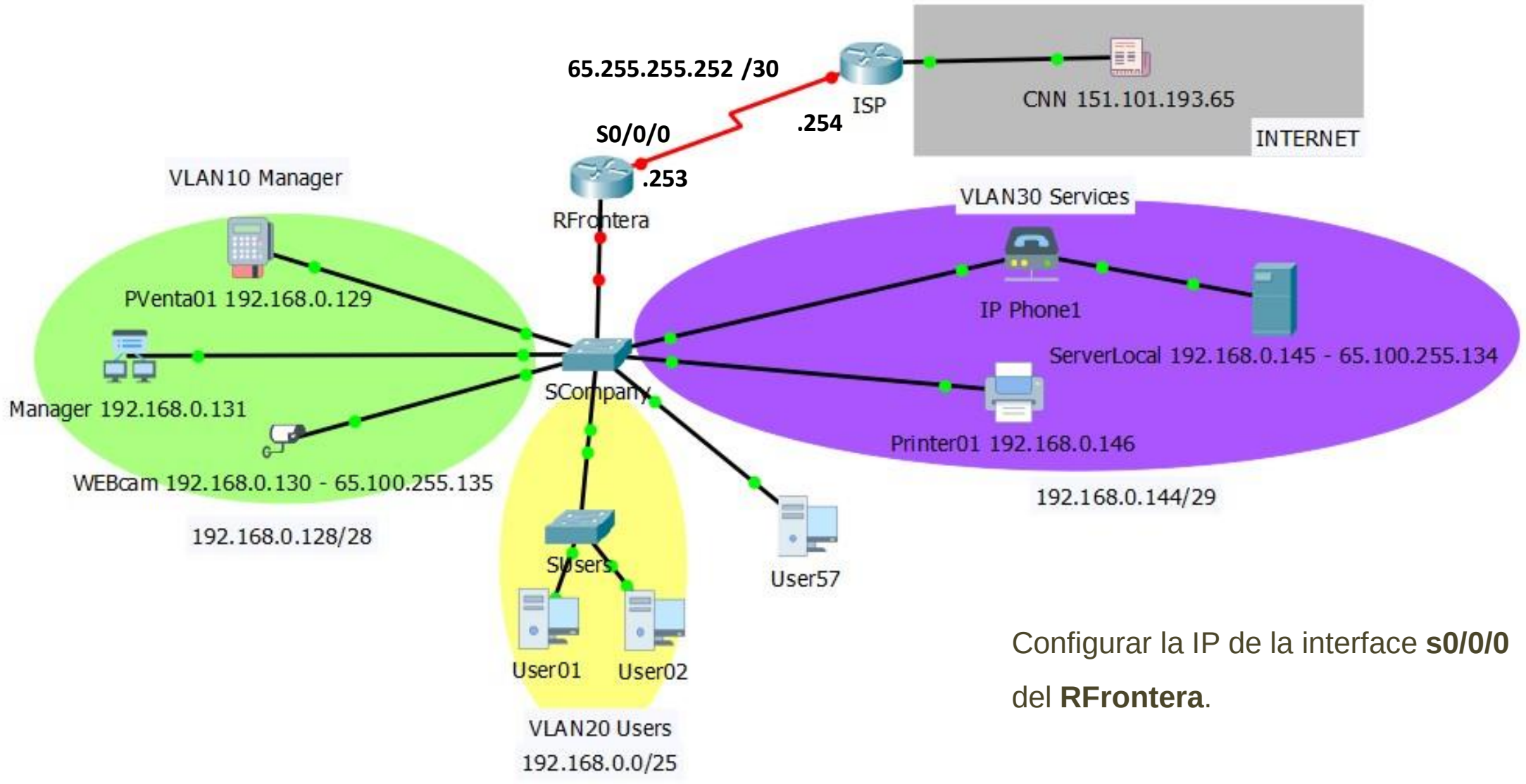
   ip nat inside (Para todas las interfaces internas de nuestra red local)

   interface Tipo-Número

   ip nat outside (Para la interface que se conecta con el exterior ISP)

Configuración de NAT

Direccionamiento público: 65.100.255.128 /29



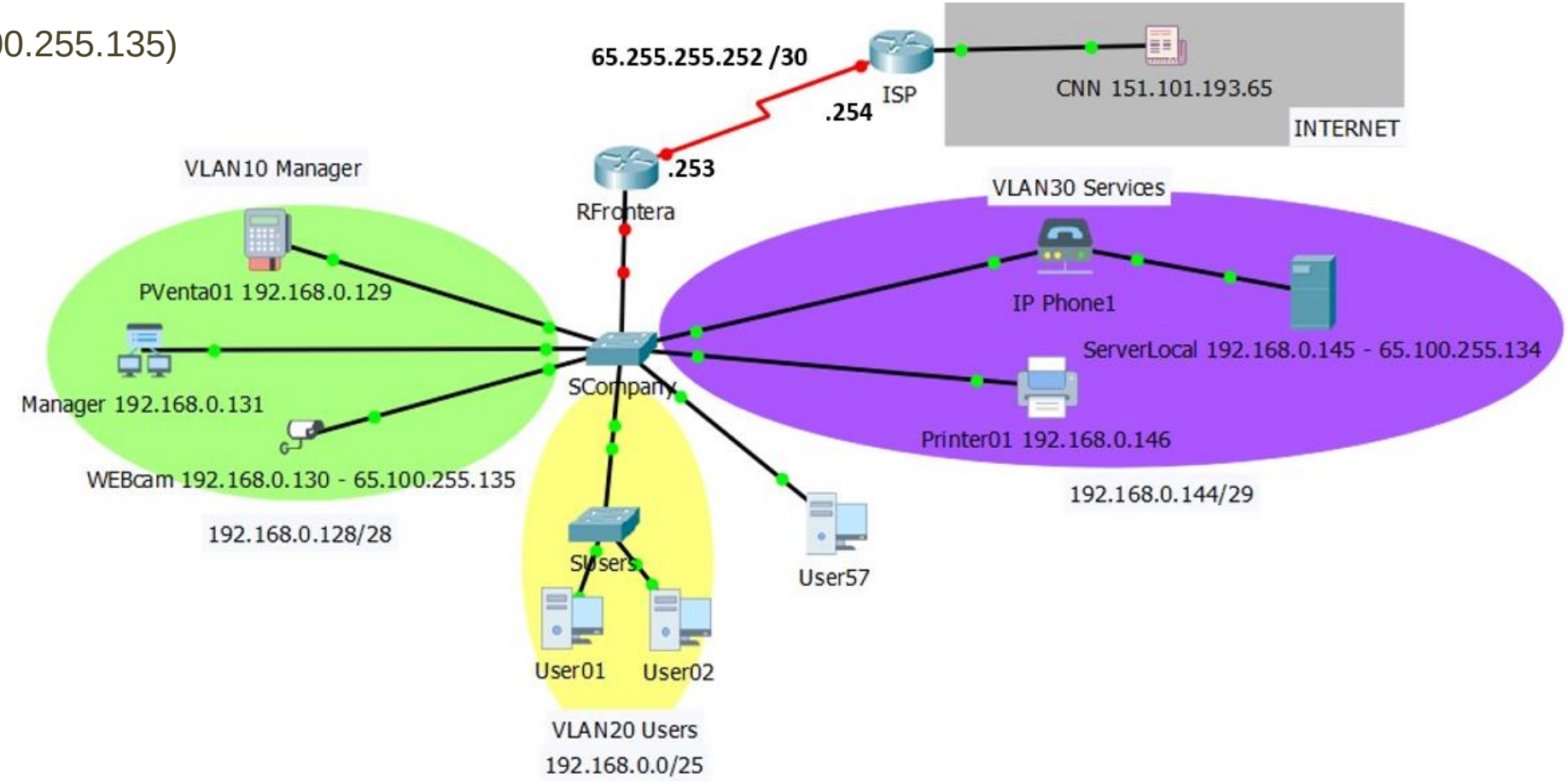
Configurar la IP de la interface **s0/0/0** del **RFrontera**.

Configuración de NAT estático

Direccionamiento público: 65.100.255.128 /29

Cuando el direccionamiento es público en el NAT todas las direcciones se pueden utilizar: **65.100.255.128 – 65.100.255.135**

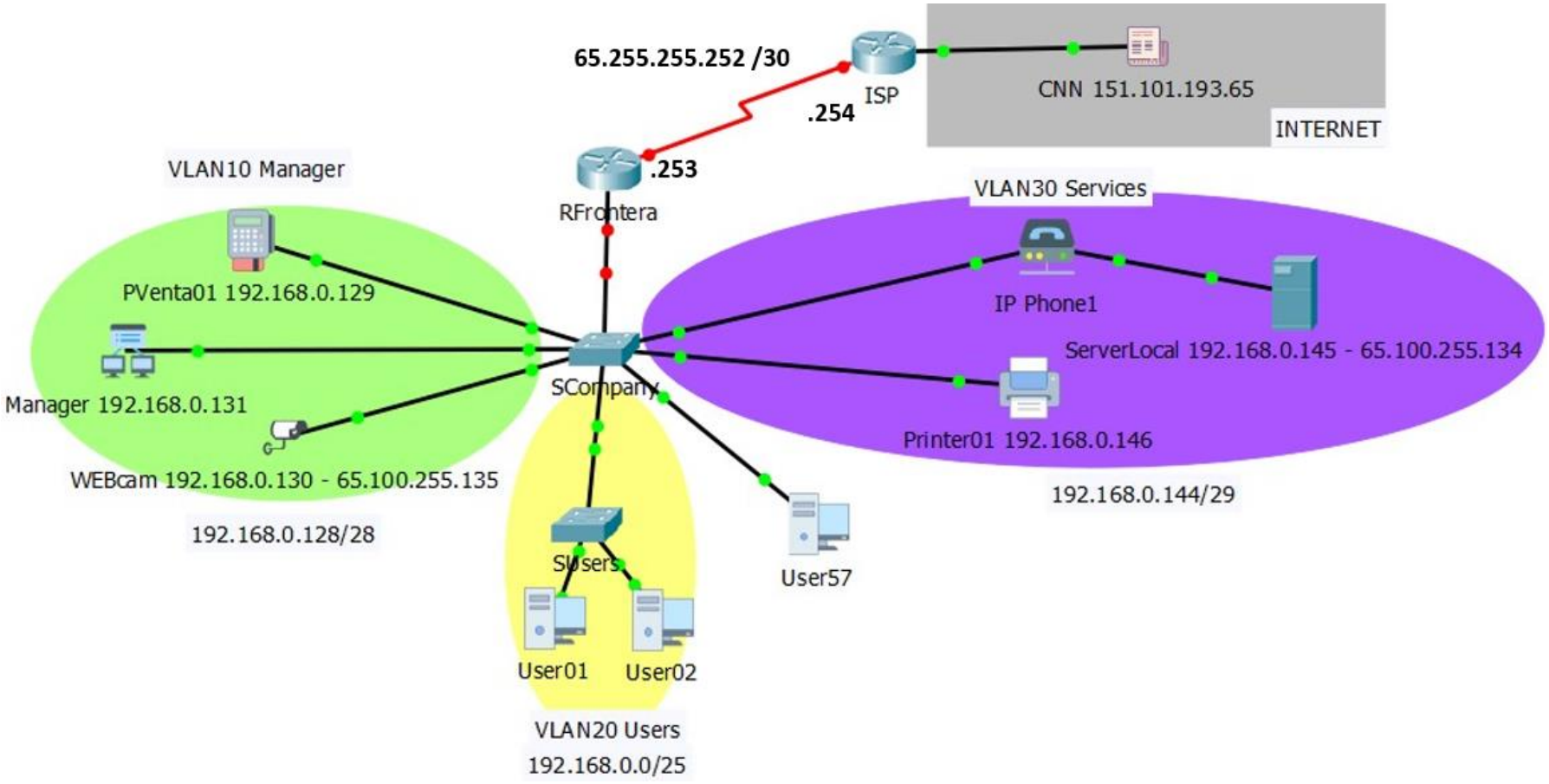
1. Configurar el **nateo estático**:
    - **Servidor Local** (65.100.255.134)
    - **Cámara web** (65.100.255.135)



Configuración de NAT con sobrecarga (PAT)

Direccionamiento público: 65.100.255.128 /29

2. Configurar **nat dinámico con sobrecarga**, ya que tenemos que traducir muchas direcciones IP privadas con pocas direcciones IP públicas.



Pruebas de conectividad

1. Probar servicio de **DHCP**.
2. Probar la conectividad interna: **interconexión entre VLANs**.
3. Probar la conectividad externa: **el servicio de NAT con sobrecarga**.
4. Probar el **NAT estático**. Probar desde el exterior el acceso al **servidor (65.100.255.134)** y a la **cámara web (65.100.255.135)**.