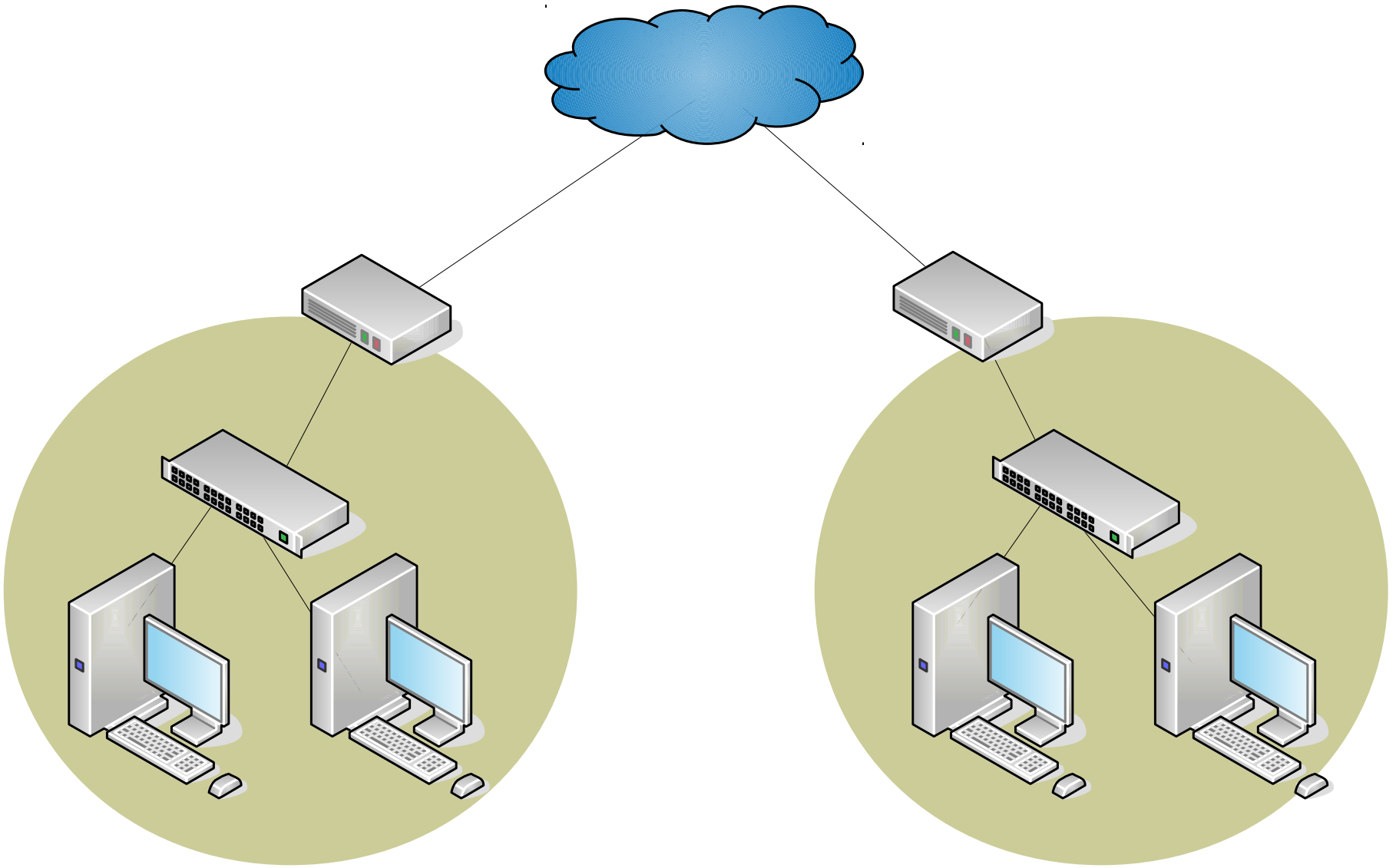
Servicios en la LAN

- LAN con direcciones privadas + NAT
- Servidores internos de WWW, Mail, archivos, con acceso desde el exterior
- Port forwarding
  - `#iptables -A PREROUTING -t nat -i eth0 -p tcp --dport 80 -j DNAT --to 192.168.1.2:8080`
  - `#iptables -A FORWARD -p tcp -d 192.168.1.2 --dport 8080 -j ACCEPT`
- Poco flexible
  - Varias sedes de la organización
  - Trabajo colaborativo
  - Seguridad
  - Varios servicios
  - Servicios dinámicos

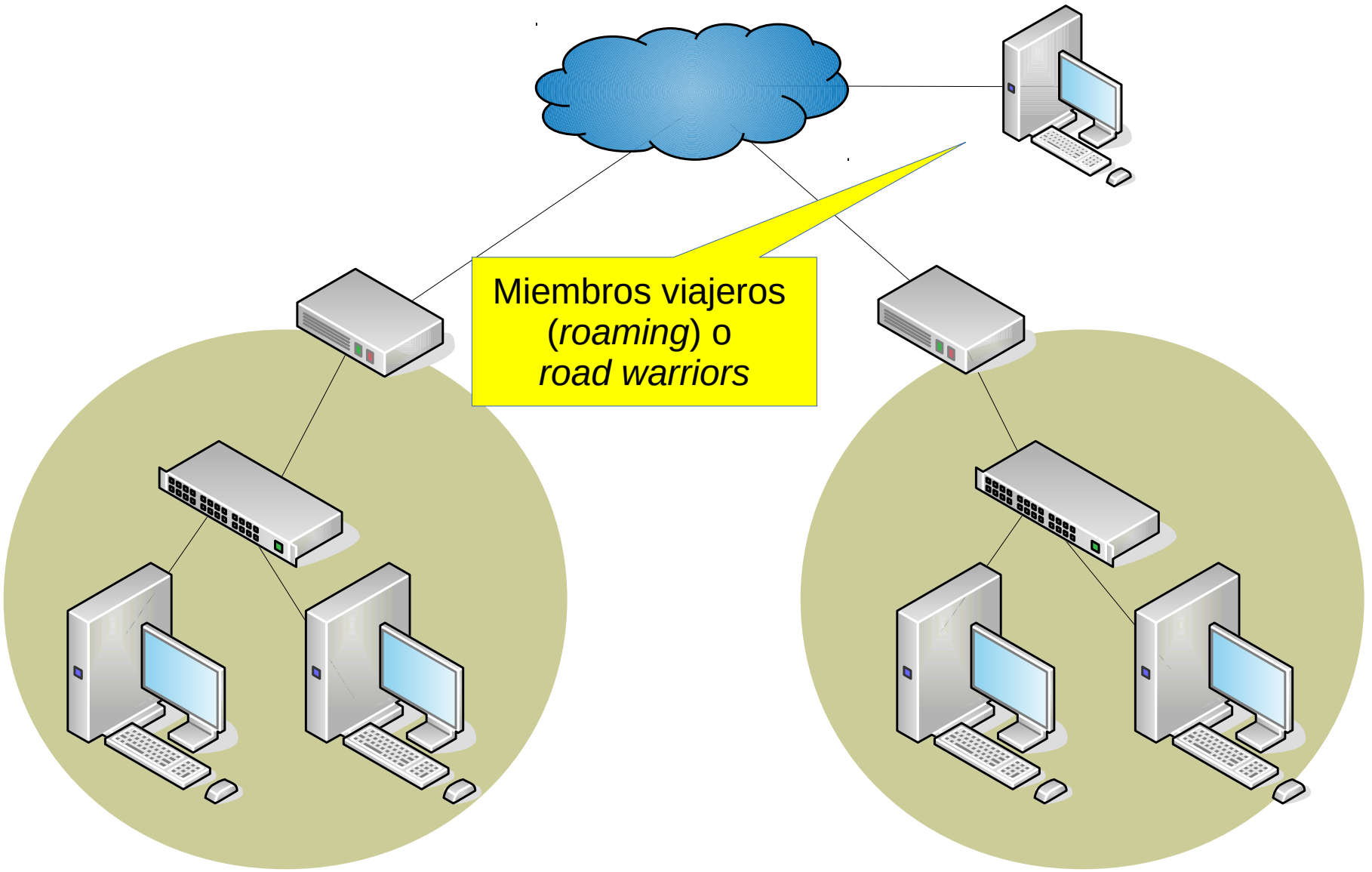
VPNs

- Redes virtuales Privadas (*Virtual Private Networks*)
- Tunneling o encapsulamiento de ciertas capas en otras
- Varios modelos e implementaciones
  - Prestadores de servicios (ISP)
  - Usuarios
  - IPSec, SSH/SSL, IP/IP
- OpenVPN

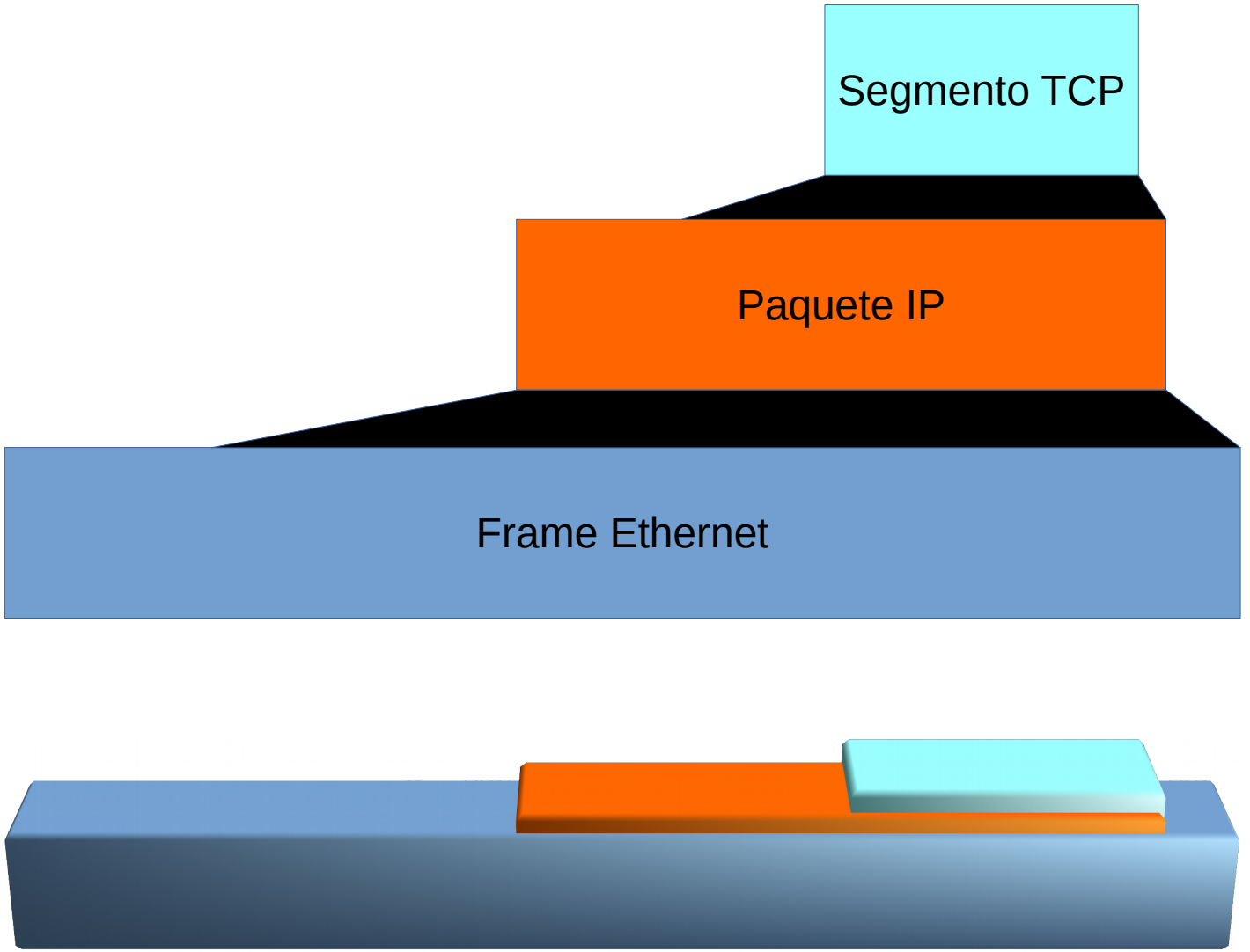
Organización con sedes



Organización con sedes

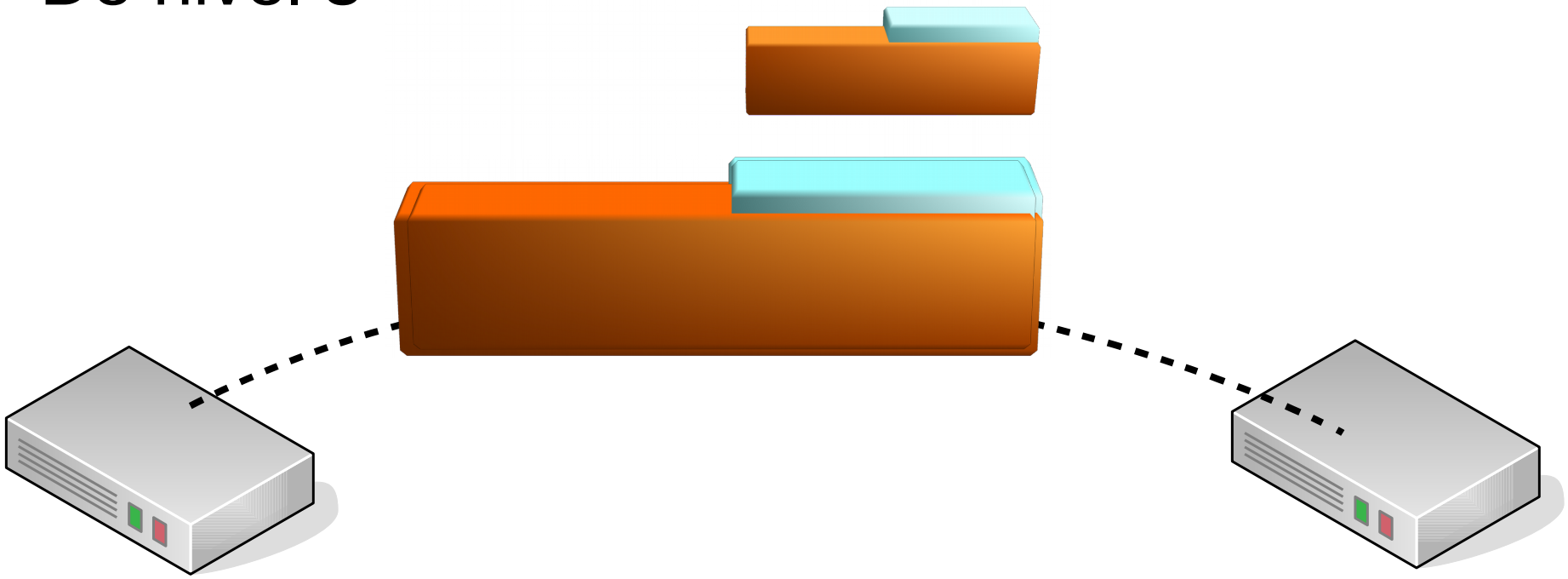


Encapsulamiento



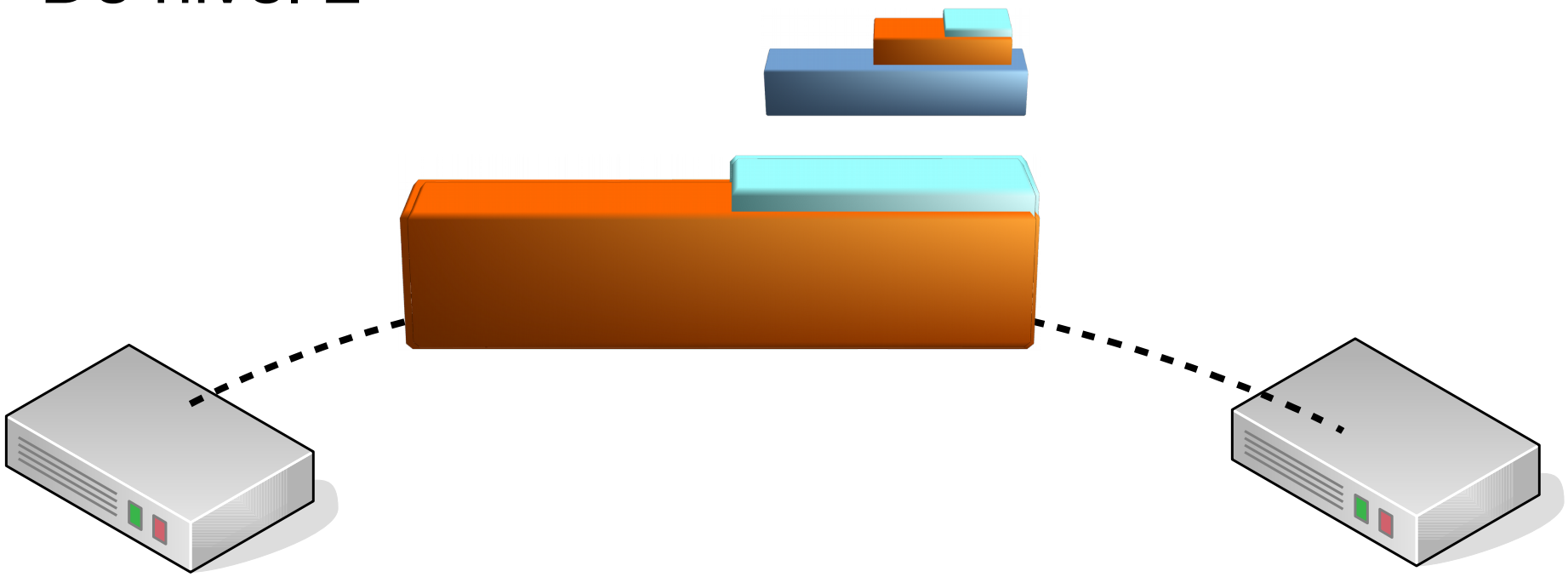
Tunneling

- De nivel 3

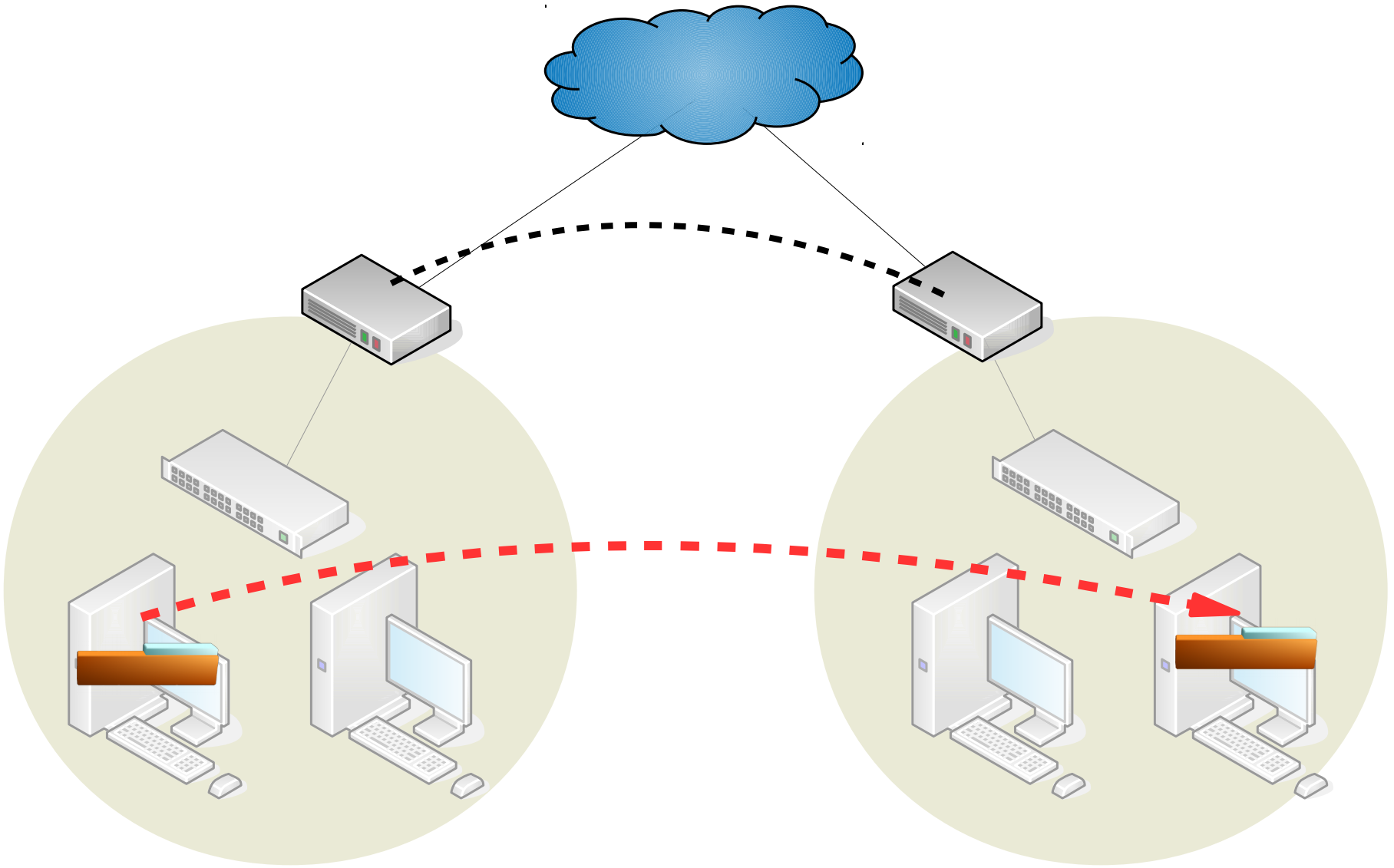


Tunneling

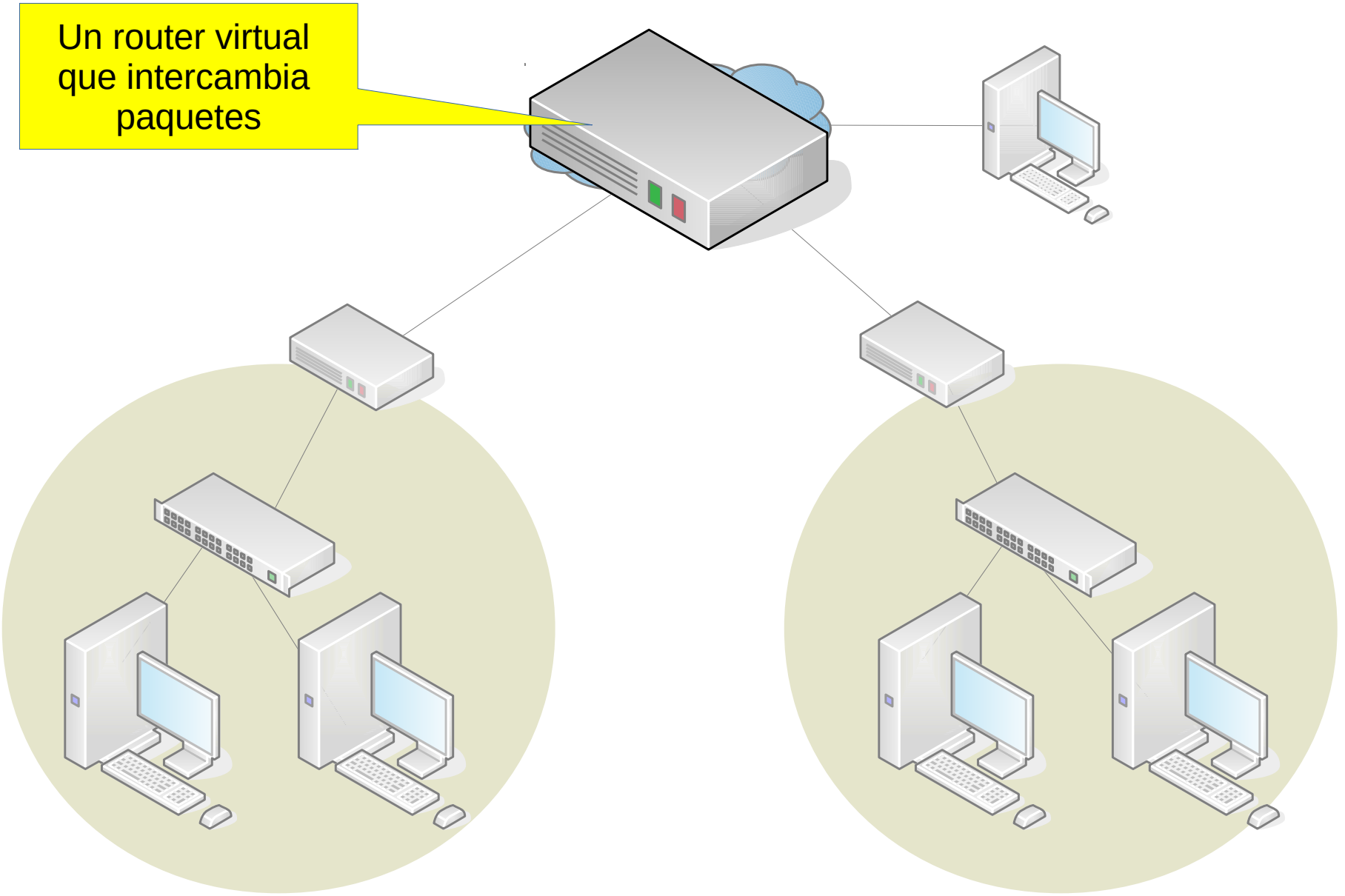
- De nivel 2



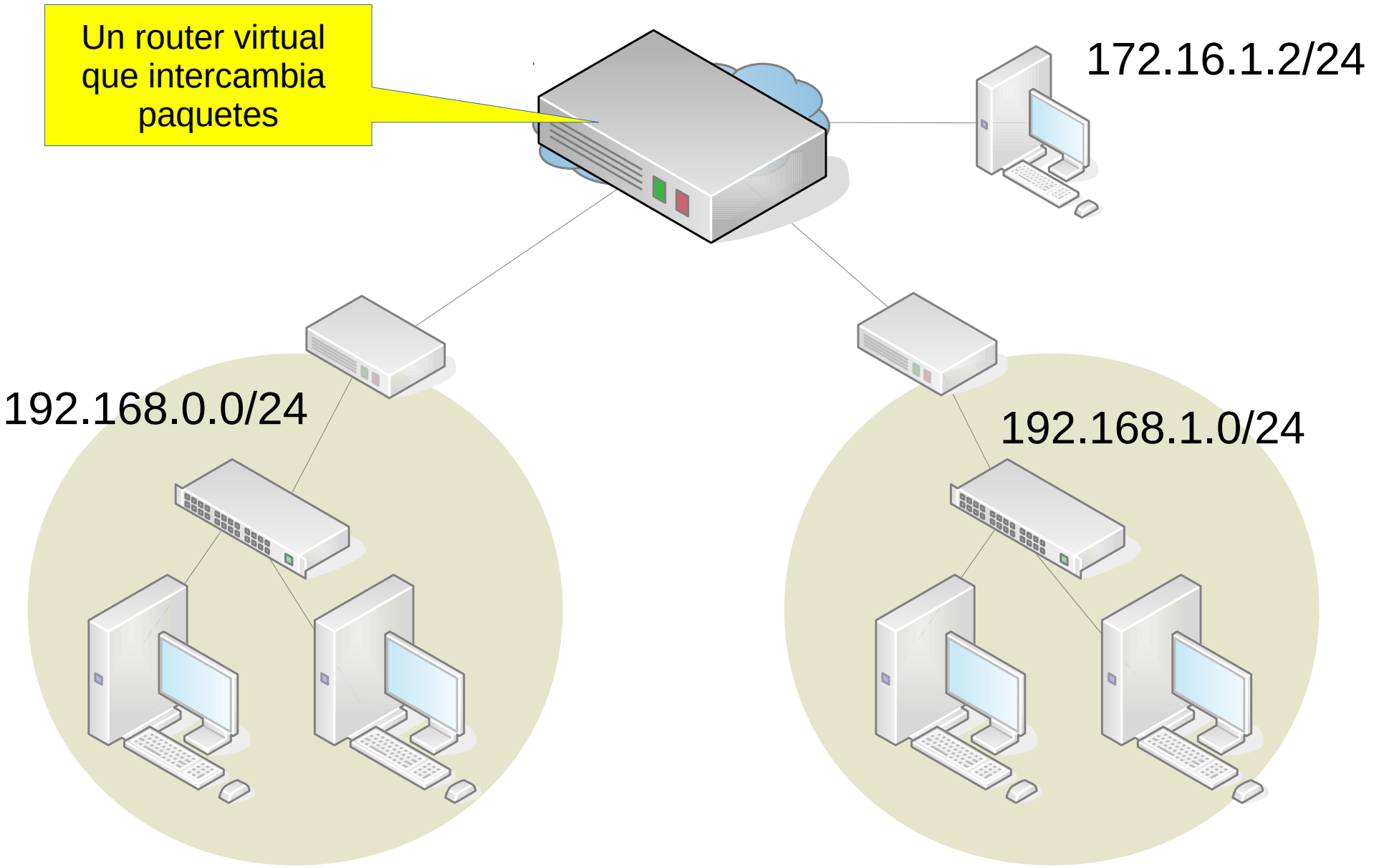
Tunneling



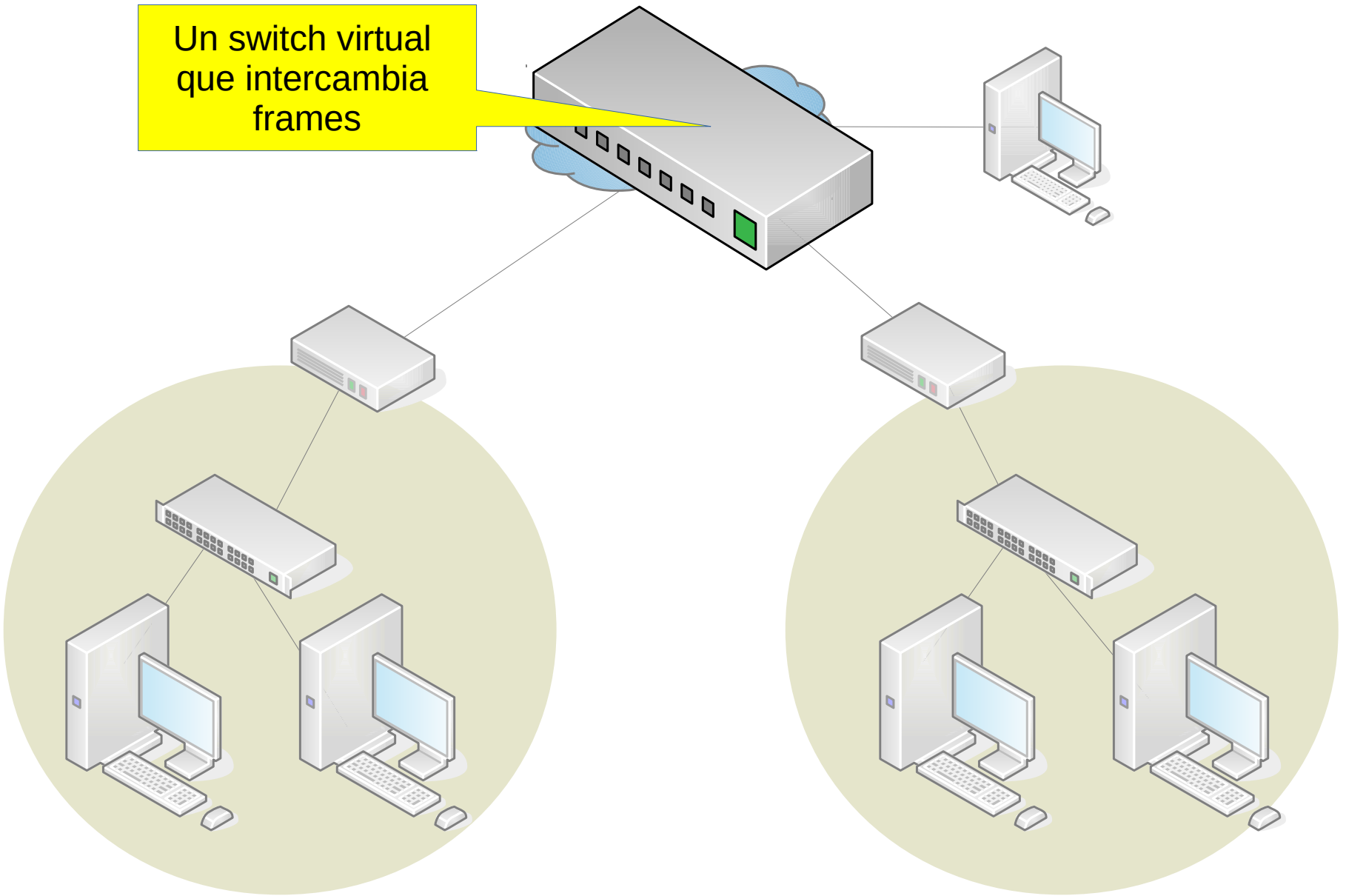
VPN de nivel 3



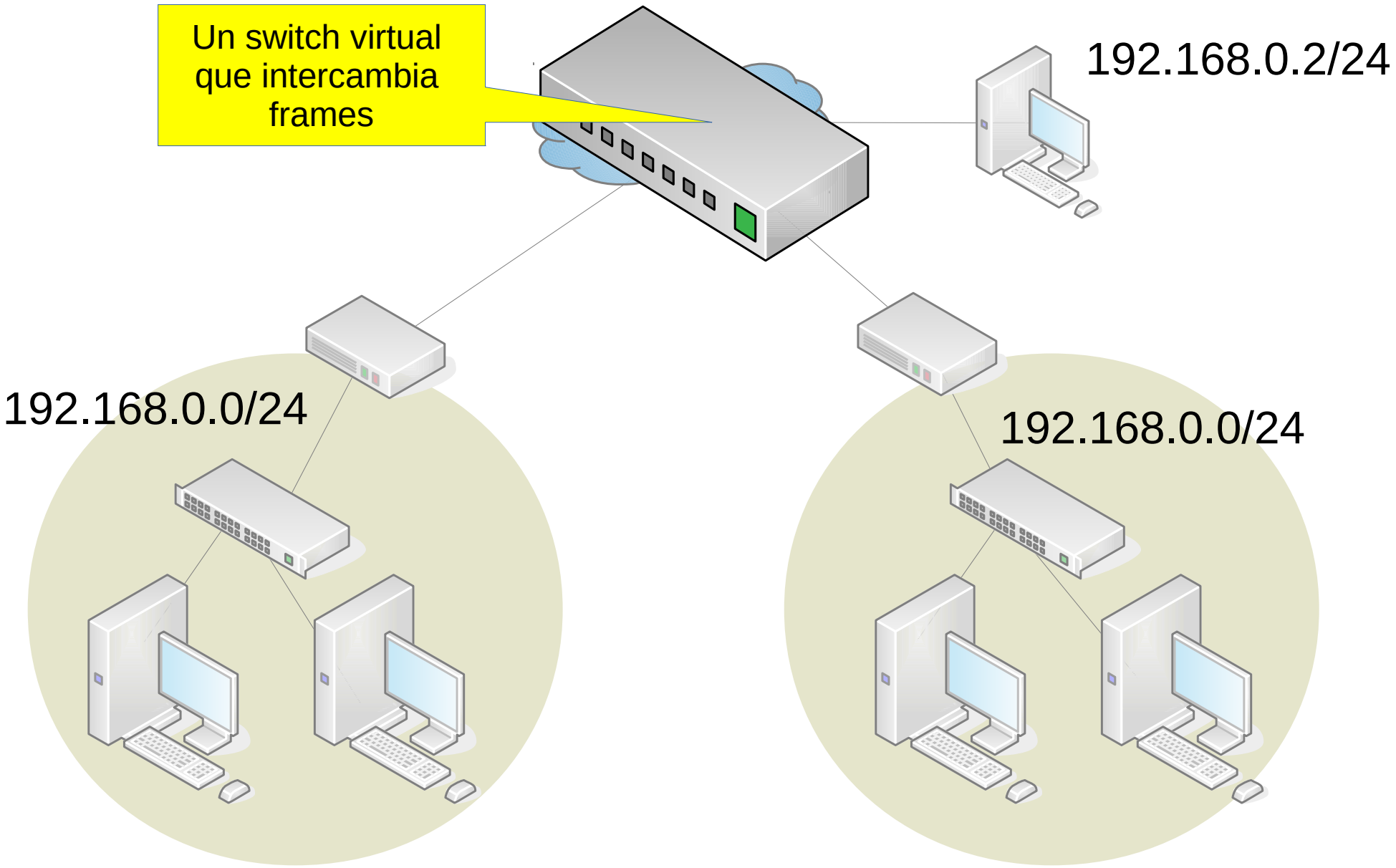
VPN de nivel 3



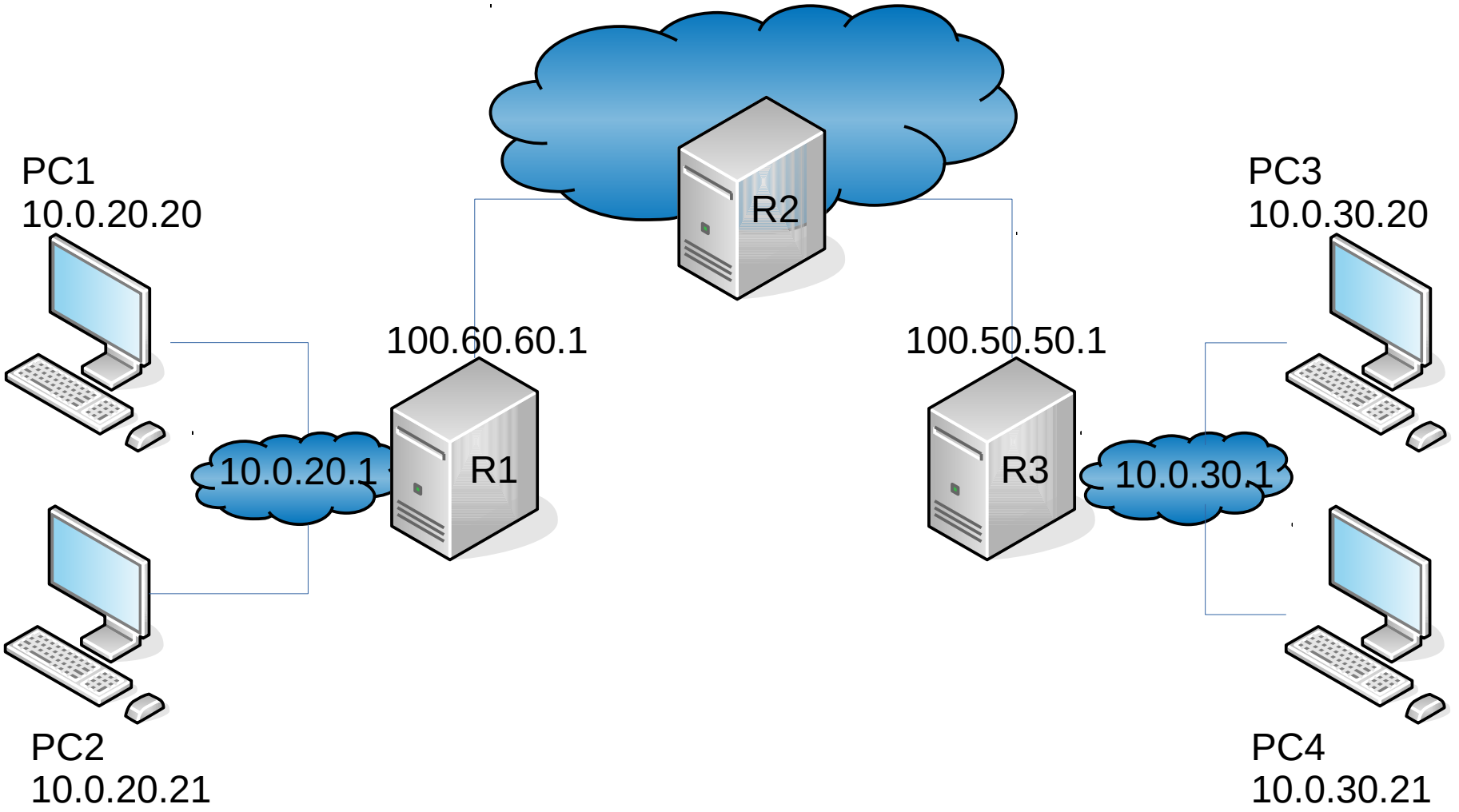
VPN de nivel 2



VPN de nivel 2



Laboratorio Openvpn L3



Laboratorio OpenVPN L3

- El router r1 funcionará como servidor y r3 como cliente
- El objetivo es tener acceso completo desde una LAN a la otra en ambos sentidos
- FASE 1: NetGUI
  - /export/home/extras/netkit/start.sh
  - Replicar el diagrama del Laboratorio
  - Configurar IP, rutas, etc. sin modificar ruteo en R2
  - ¿Se accede desde una LAN a la otra? ¿Qué parecido tiene esta situación con Internet?
- Fase 2: Obtener configuración
  - Descargar openvpn-lab.tgz al home
  - cp /hosthome/openvpn-lab.tgz /etc/openvpn

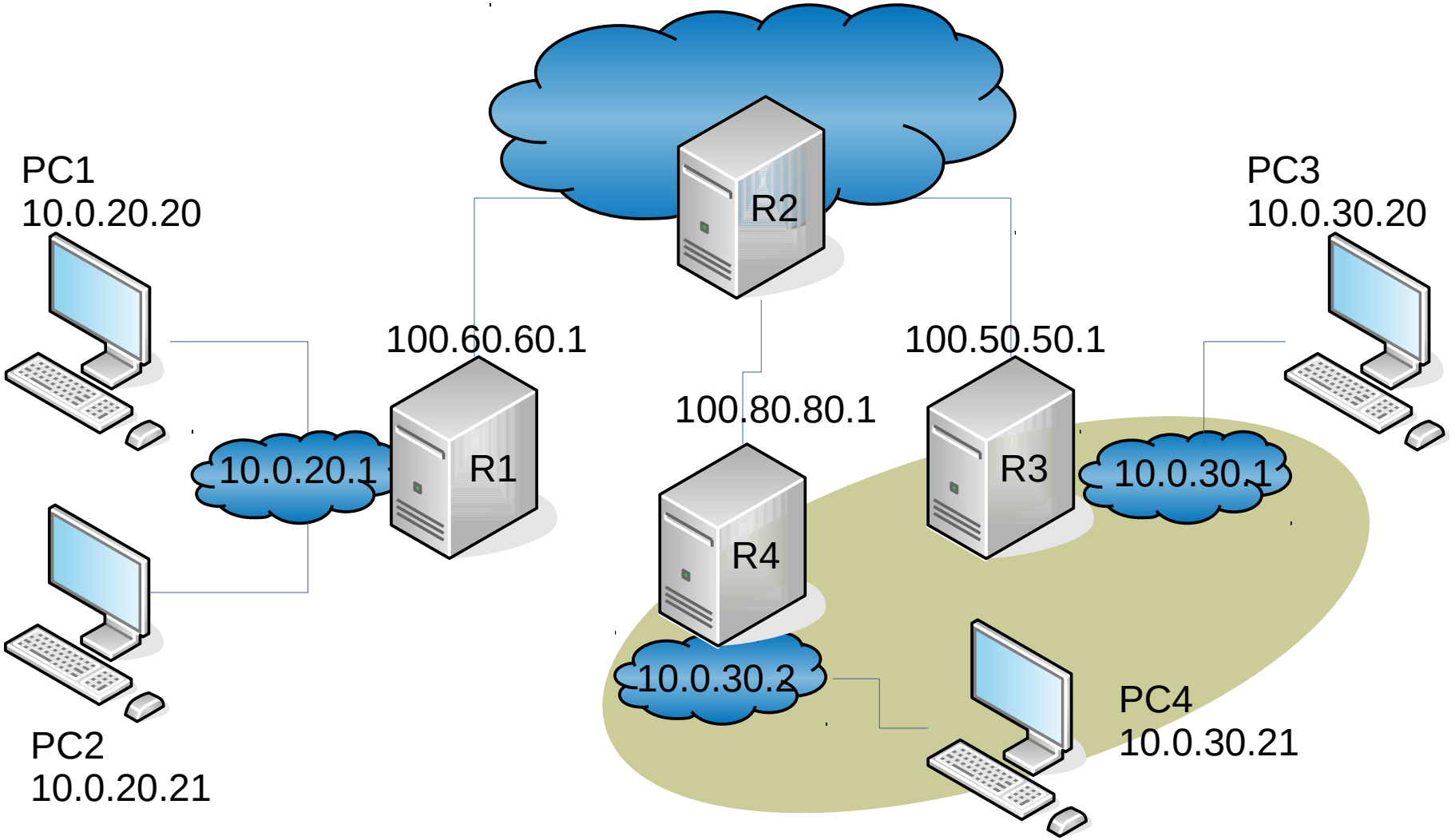
Laboratorio OpenVPN L3

- Fase 3
  - Utilizar las configuraciones de cliente y servidor dadas
  - Comprobar que se establece la conexión entre ambos
  - ¿Se accede desde una LAN a la otra?
- Fase 4
  - Agregar detalles de ruteo en el servidor
  - Comprobar que una LAN accede a la otra y viceversa
- Fase 5
  - Instalar el paquete easy-rsa
  - Definir una CA y generar certificados para CA, r1 y r2
- Fase 6
  - Instalar un segundo cliente, r4
  - Comprobar que todas las LANs se acceden mutuamente

Configuración de ruteo L3

- Publicar redes detrás del servidor
  - `push “route RED-LOCAL MASCARA”`
    - Inyecta una nueva ruta en los clientes
- Incorporar a la VPN redes detrás de clientes
  - `client-config-dir clients`
  - `route RED-REMOTA MASCARA`
  - En `/etc/openvpn/clients/nombrecliente:`
    `iroute RED-REMOTA MASCARA`
    - Incorpora en el servidor rutas a las redes remotas

Laboratorio OpenVPN L2/L3

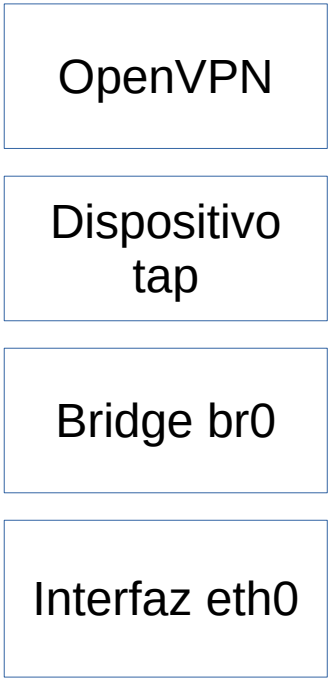


Laboratorio OpenVPN L2/L3

- En este laboratorio se creará una configuración mixta con dos procesos OpenVPN en capas 3 (Red) y 2 (Enlace)
- El objetivo es tener acceso completo entre las tres redes, pero conformando un único dominio de broadcast entre las redes de r3 y r4
- El router r1 funcionará como servidor y r3 como cliente de una VPN de nivel 3
  - Misma experiencia que se ha hecho en el laboratorio anterior
  - Ambas redes locales tienen direcciones sobre redes IP diferentes
  - La VPN conducirá paquetes IP entre sus redes
- A su vez, el router r3 será servidor, y r4 cliente, de una VPN de nivel 2
  - Ambas redes locales tienen direcciones sobre la misma red IP
  - La VPN conducirá frames Ethernet entre ambas redes

Configuración Lab L2/L3

- Se necesita un segundo archivo de configuración server-l2.conf en r3
  - Directiva server-bridge
  - Dispositivo tap
- Archivo de configuración cliente-l2.conf en r4
- Documento de la materia, Anexo Scripts para OpenVPN en modo bridge



Configuración Lab L2/L3