

Práctica 1.

Configuración de red:

routing y firewalls

Roberto Magán Carrión

FR - GII

✉ rmagan@ugr.es



UNIVERSIDAD
DE GRANADA

Objetivos

- Laboratorio 3.7
- Fundamentos de *routing* (*estático y dinámico*) y configuración.
- *Firewalls* y filtrado de paquetes IP.

Laboratorio 3.7

Puestos de trabajo

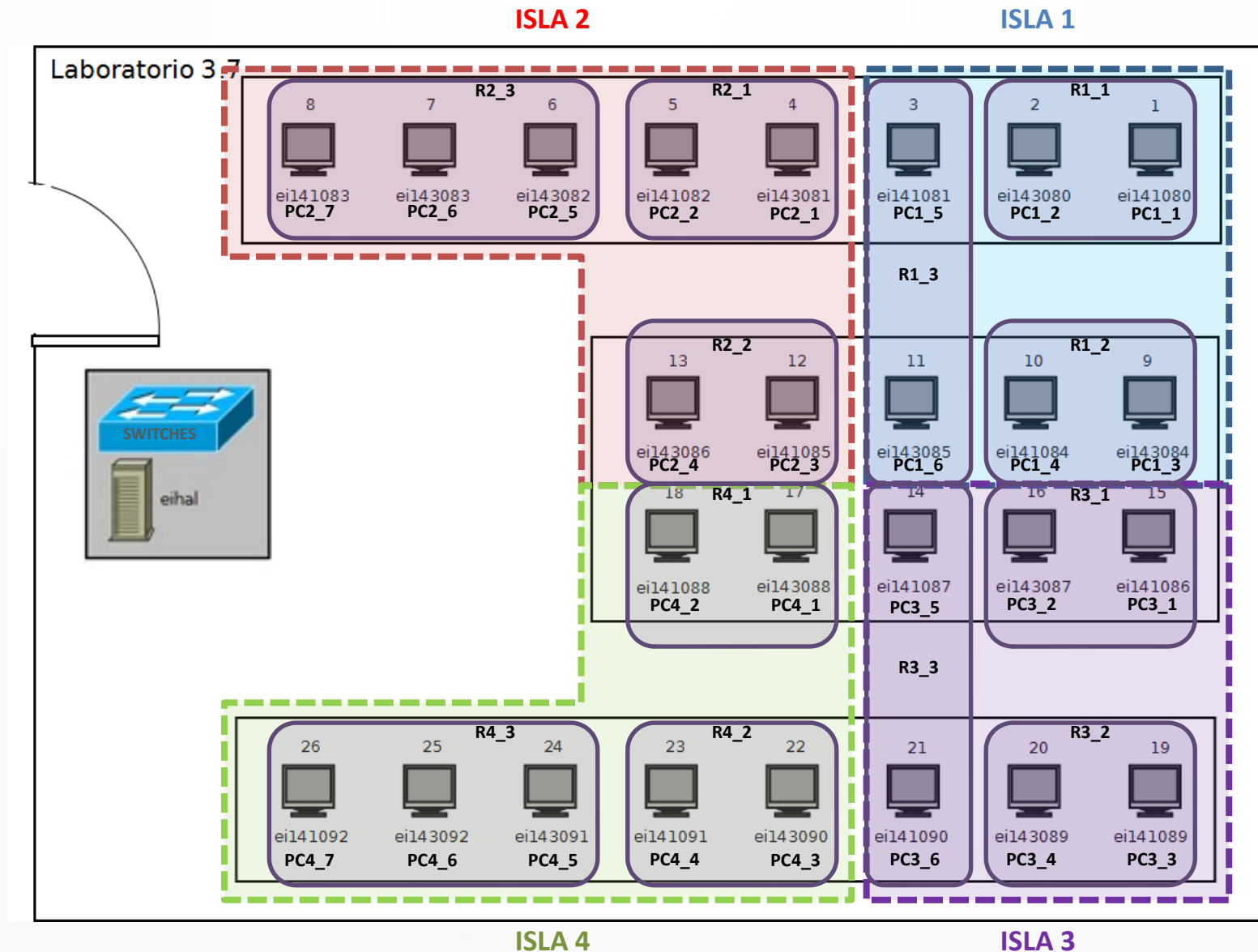
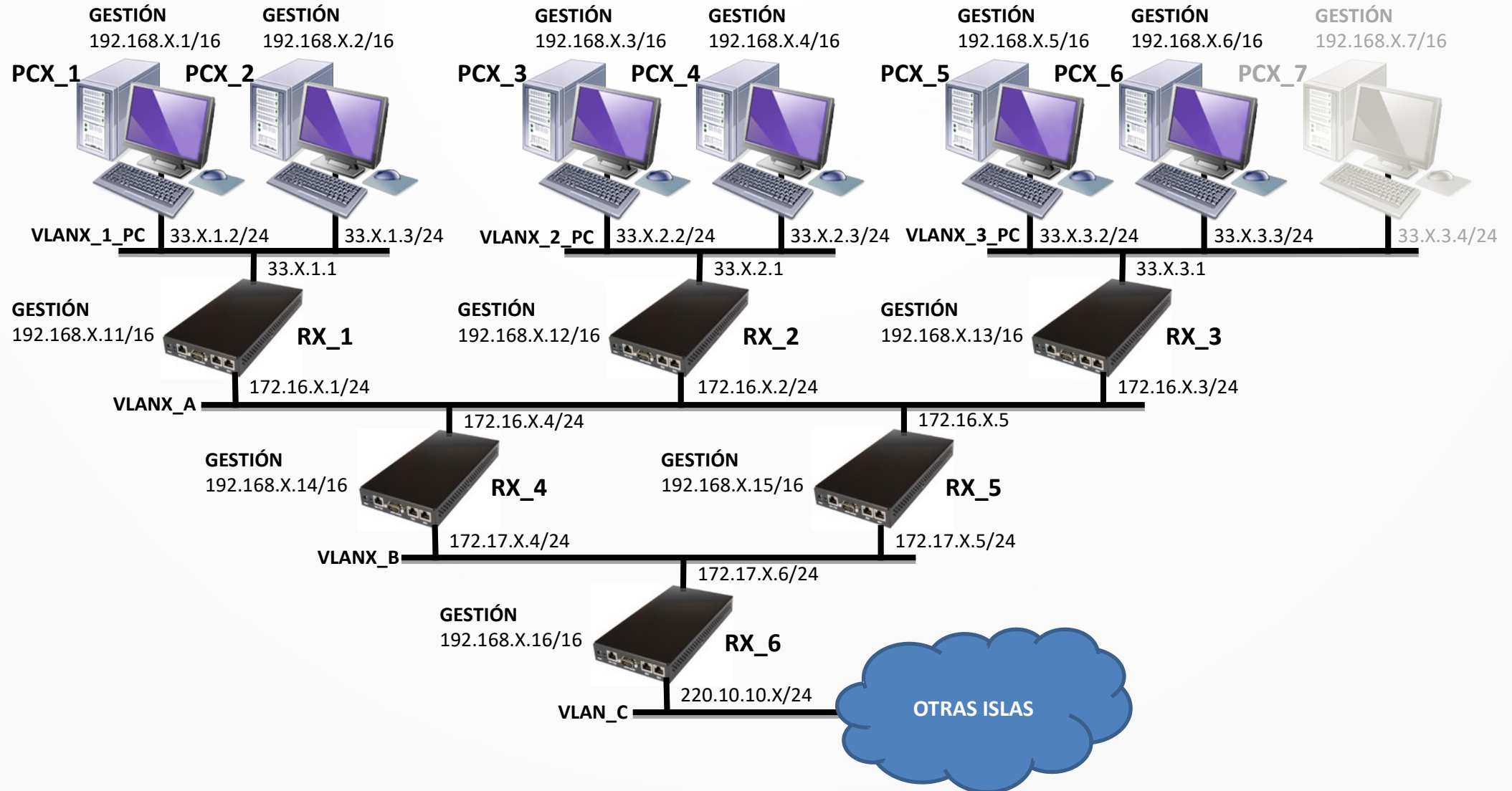


Diagrama lógico de red



Fundamentos de encaminamiento (routing) IP y reenvío de paquetes

Encaminamiento (*routing*) IP

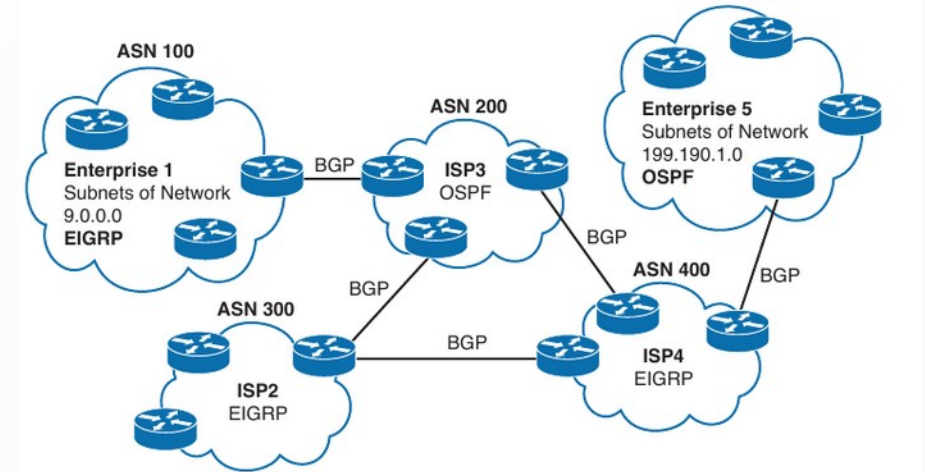
- **Estáticos**

- i Basados en la configuración manual de tablas de encaminamiento.
- ii No se adaptan a los cambios en la topología de la red.

- **Dinámicos**

- i Basado en **protocolos de routing**¹:
 - *Aprendizaje y difusión de rutas*
 - *Cálculo de la ruta más corta al destino (métricas)*
 - *Convergencia*
- ii Tipos:
 - *IGP (Interior Gateway Protocol) → **RIP**, OSPF, etc.*
 - *EGP (Exterior Gateway Protocol) → BGP*
- iii Se adaptan a los cambios en la topología de la red.

Destino	Próximo salto (GW)
33.1.2.0/24	-
33.1.1.0/24	-
200.20.20.0/30	172.16.1.2
0.0.0.0	192.168.1.1



¹Un protocolo de routing se compone de un conjunto de normas, mensajes y algoritmos utilizados para el aprendizaje de rutas. Las mejores rutas se establecen en las tablas de encaminamiento de los routers.

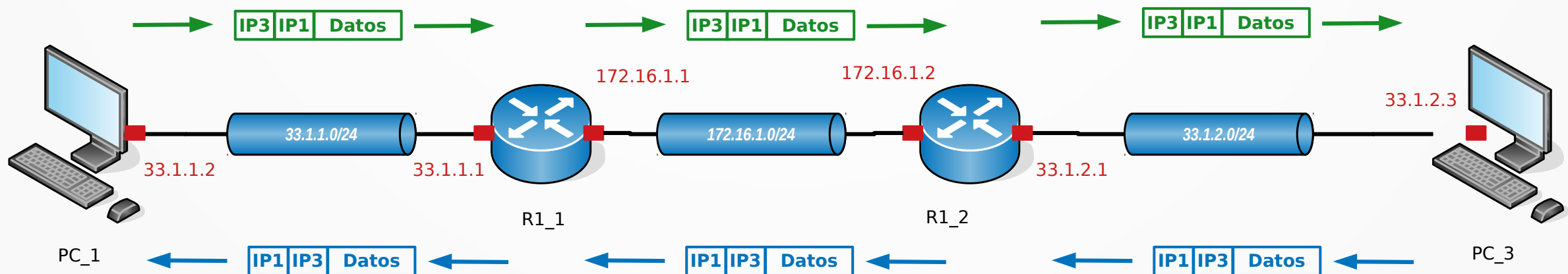
Reenvío y *routing*

Routing estático

Destino	Próximo salto (GW)
0.0.0.0/0	33.1.1.1
33.1.1.0/24	-

Destino	Próximo salto (GW)
0.0.0.0/0	33.1.2.1
33.1.2.0/24	-

PETICIÓN



Destino	Próximo salto (GW)
33.1.2.0/24	172.16.1.2
33.1.1.0/24	-

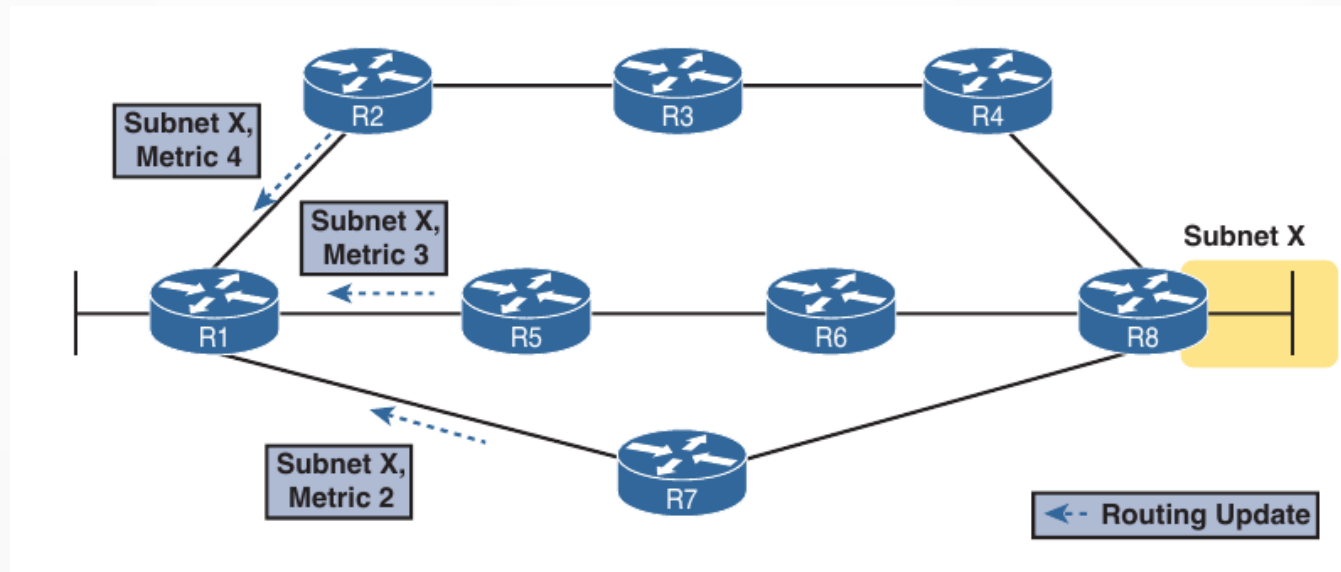
Destino	Próximo salto (GW)
33.1.1.0/24	172.16.1.1
33.1.2.0/24	-

RESPUESTA

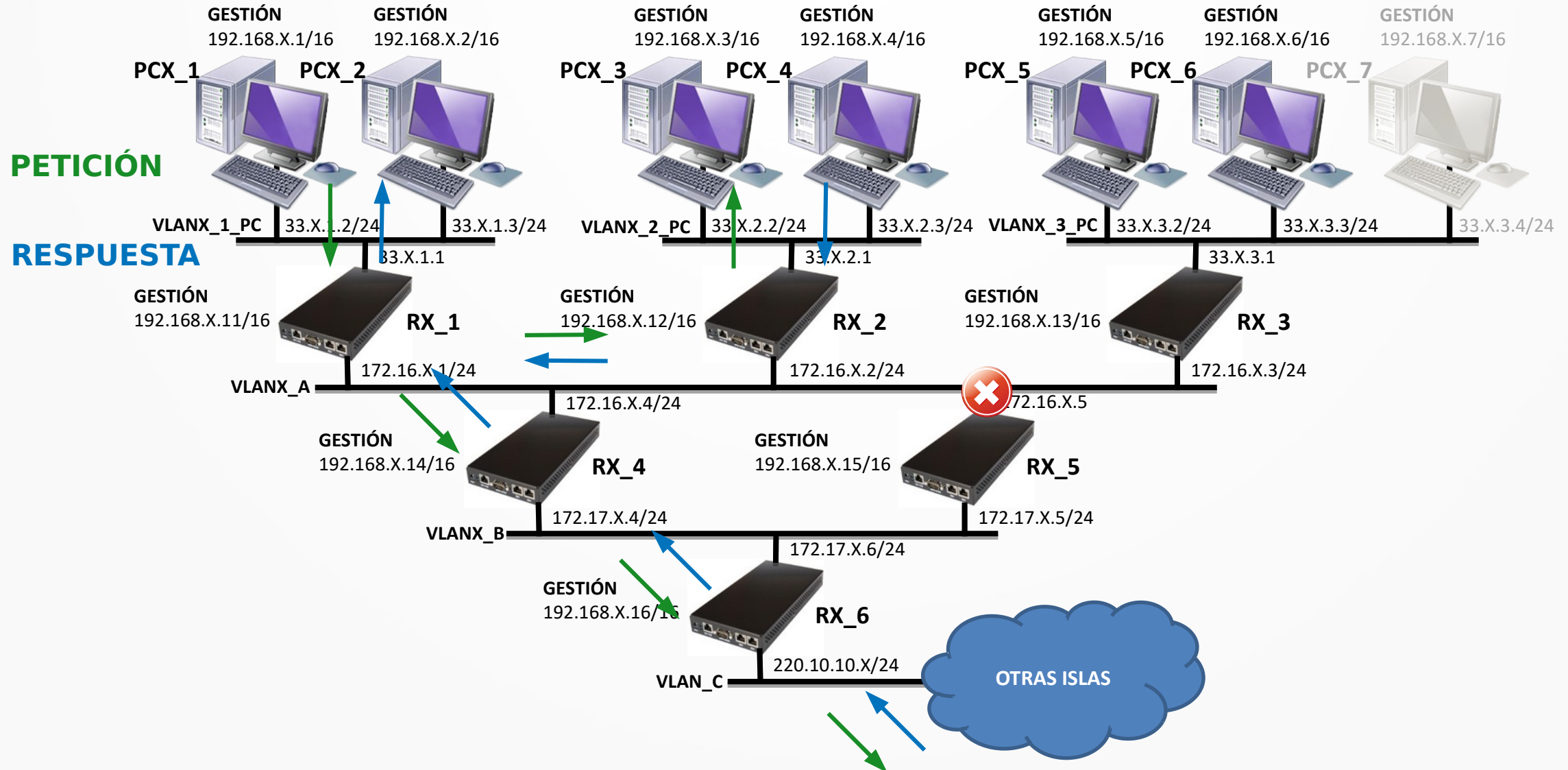
Reenvío y *routing*

Routing dinámico: RIP (Routing Information Protocol)

- Distance Vector (DV)
 - i DV: [destino, métrica, *next-hop*]
 - ii Actualizaciones periódicas (30s)
 - iii Convergencia lenta
 - iv Redes pequeñas (máximo 15 saltos)



Escenario práctico



To take away ...



- **Usar pasarelas por defecto cuando proceda**

- i Pasarela por defecto: Todo el tráfico que no va dirigido a mi subred, lo envío siempre por un único camino.
- ii *Routers* → `0.0.0.0/0 | <IP-pasarela-gateway>`
- iii *PC* → `sudo route add default gw <IP-pasarela-gateway>`



- **Encaminamiento salto a salto**

- i Configurar entradas en la tablas de encaminamiento en cada salto.
- ii *PC y routers*



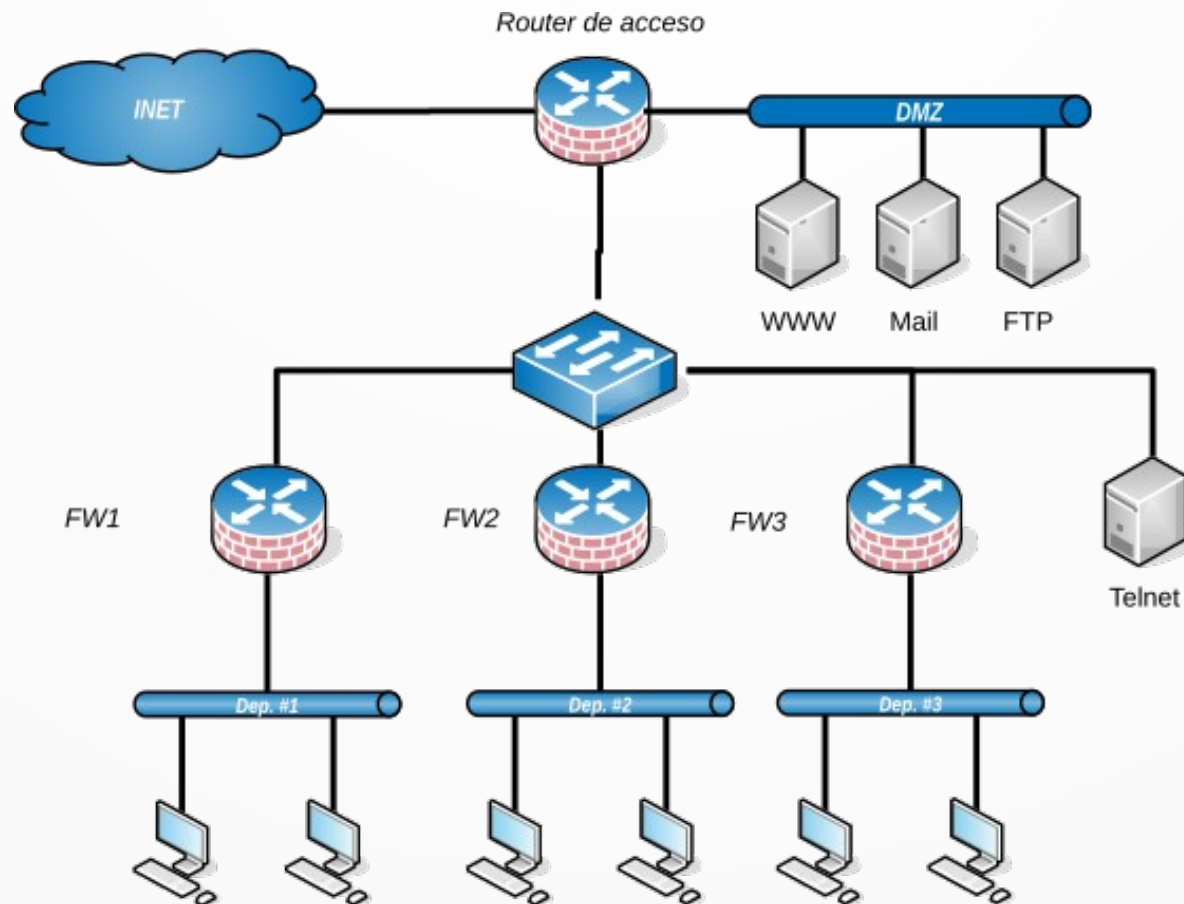
- **Comprobar conectividad**

- i `ping -R <IPdestino>`

Control de acceso y firewalls

Firewalls

Un **cortafuegos** en una red computadores consiste en una **pasarela/barrera que separa dos redes o subredes**. Normalmente una red interna (intranet) de una externa (extranet) a la organización.



Firewalls

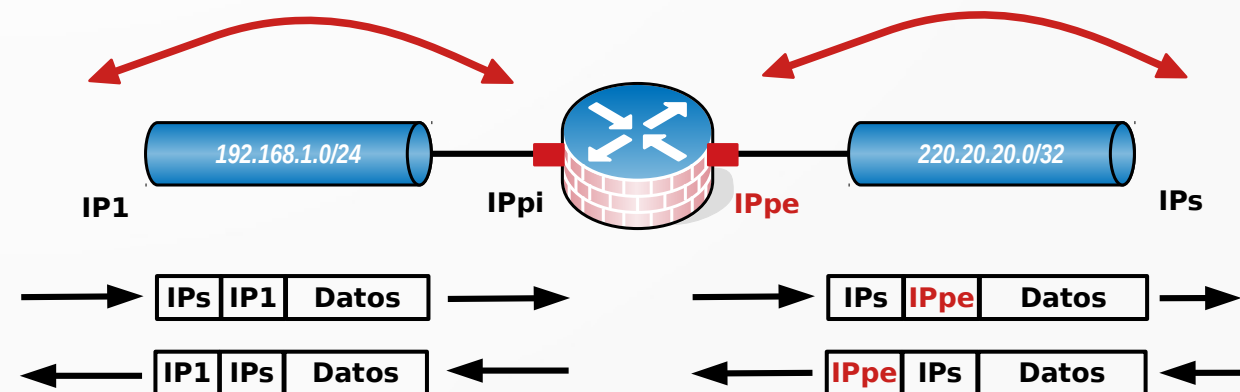
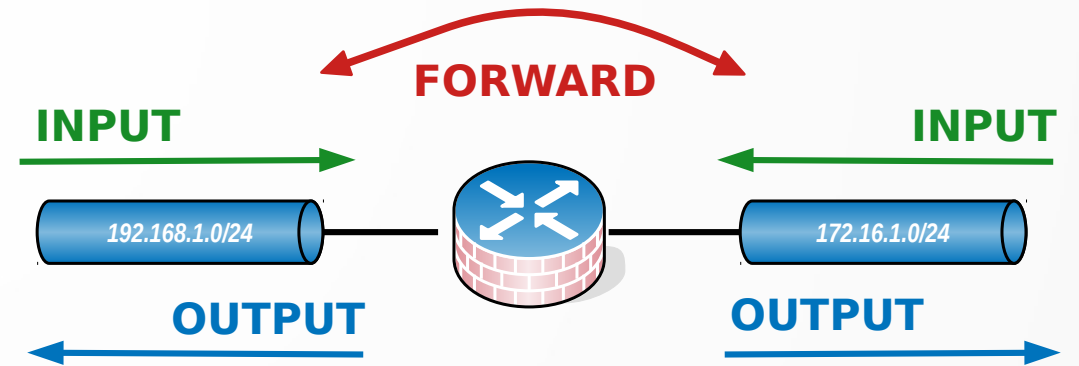
- **De filtrado**

- i Reglas de filtrado asociadas a cadenas (**INPUT**, **OUTPUT** y **FORWARD**).
- ii Acciones: *drop*, *accept*, *reject*.
- iii Filtrado por: IP origen/destino, puerto origen/destino, protocolo (TCP/UDP), etc.

```
/ip firewall filter chain=forward dst-address=33.1.1.3 action=accept
```

- **De aplicación (*proxy*)**

- i Intermediario de la conexión.



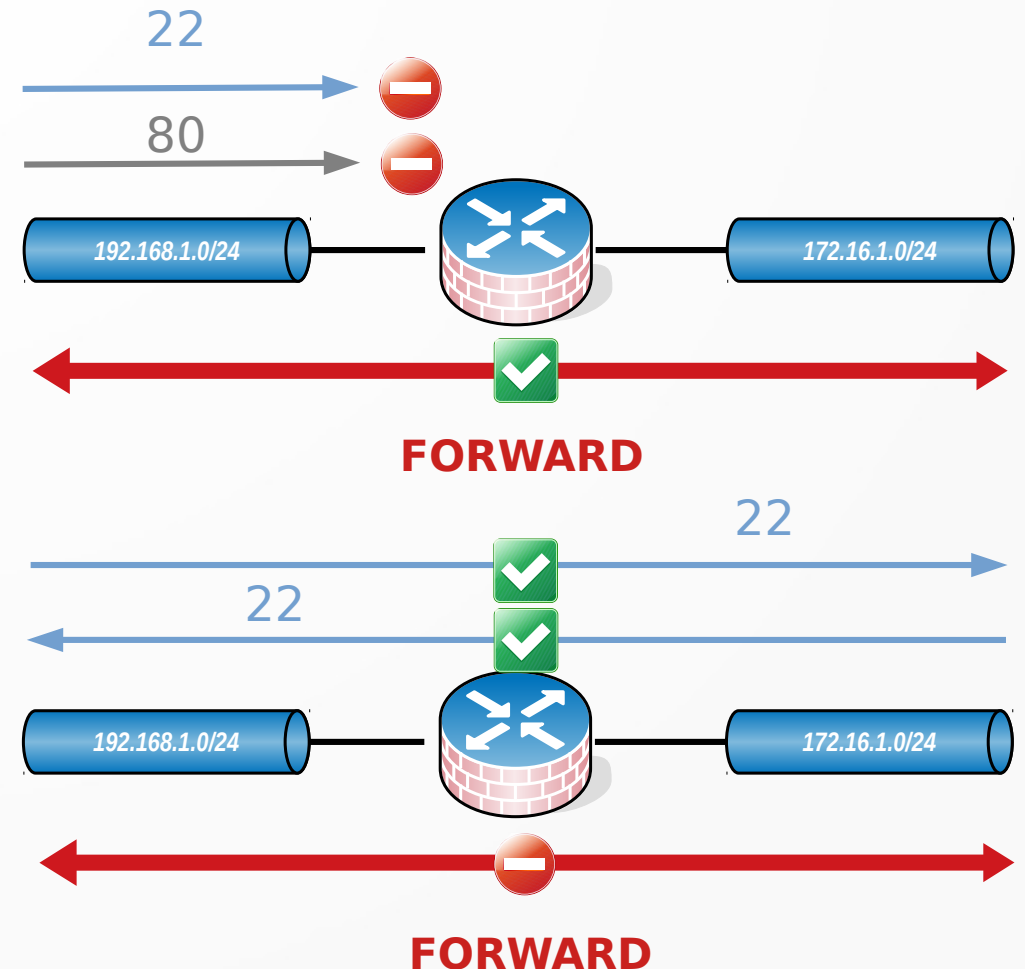
Políticas de seguridad

- Permisiva

- i Por defecto se acepta toda comunicación
- ii Se descarta (**drop**) de forma selectiva

- Restrictiva

- i Por defecto se descarta toda comunicación
- ii Se acepta (**accept**) de forma selectiva

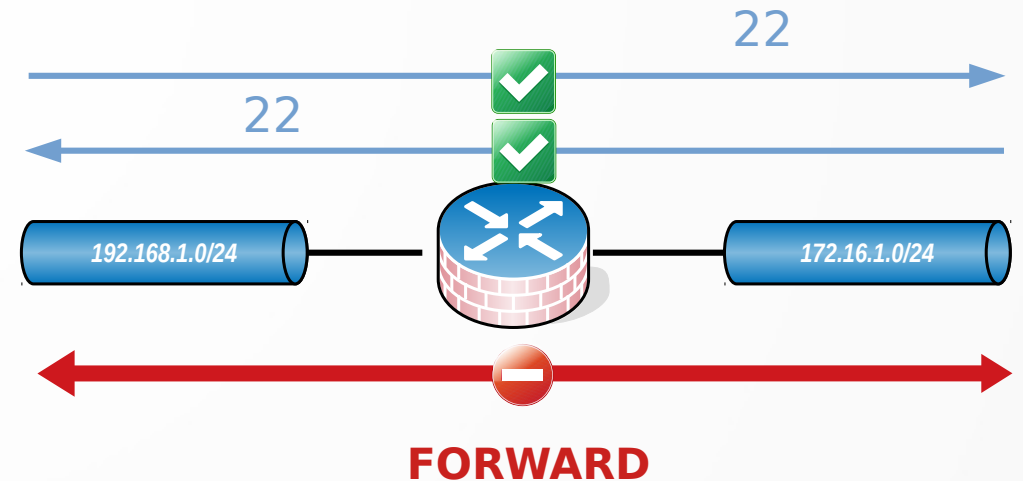


Políticas de seguridad

- **Restictiva**

- i Por defecto se descarta toda comunicación
- ii Se acepta (***accept***) de forma selectiva

- ✓ accept forward ...
- ✓ accept forward ...
- ⊖ drop forward



To take away ...



- **Solo trabajaremos sobre la cadena FORWARD**

- i El tráfico no va dirigido al *router* si se origina en el *router*.



- **NO hacer drop sobre INPUT y OUTPUT**

- i No podríamos acceder al *router* para configurarlo



- **¿Cómo vemos si una regla se está evaluando?**

- i Firewall → Filter Rules
 - ii Activar Logging para el Firewall

Firewall										
Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols										
+ - [check] [x] [filter] [00] Reset Counters [00] Reset All Counters										
#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	Bytes	Packets	
0	✓ accept	forward		33.1.2.0/24	6 (tcp)		22	180 B	3	

To take away ...



- **No dejar campos en blanco al configurar el *firewall***

Firewall Rule <>

General Advanced Extra Action Statistics

Chain:

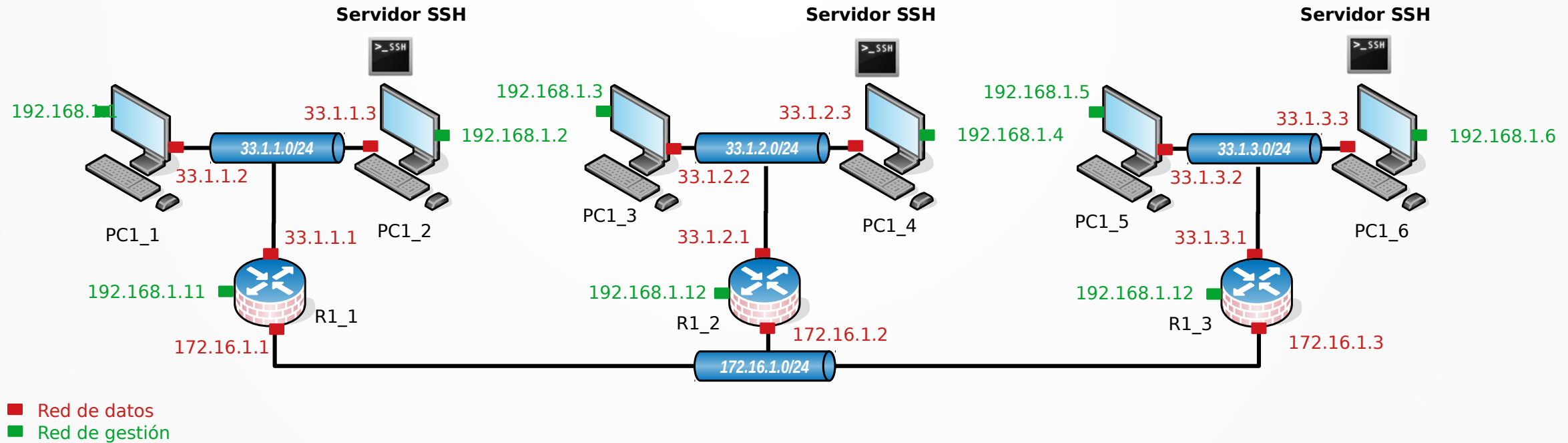
Src. Address:

Dst. Address:

Protocol: ☐ 6 (tcp)

Src. Port: ☐

Escenario práctico



- **Antes de empezar a trabajar con el *firewall*:**
 - i Configurar encaminamiento entre PC
 - ii Comprobar conectividad con *ping -R*

Práctica 3.

Configuración de red:

routing y firewalls

Roberto Magán Carrión

FR - GII

✉ rmagan@ugr.es



25

UNIVERSIDAD
DE GRANADA