

Paris Traceroute



Índice

- Introducción
- Problemas
- Soluciones
- Implementación
- Pruebas

Índice

- Introducción
- Problemas
- Soluciones
- Implementación
- Pruebas

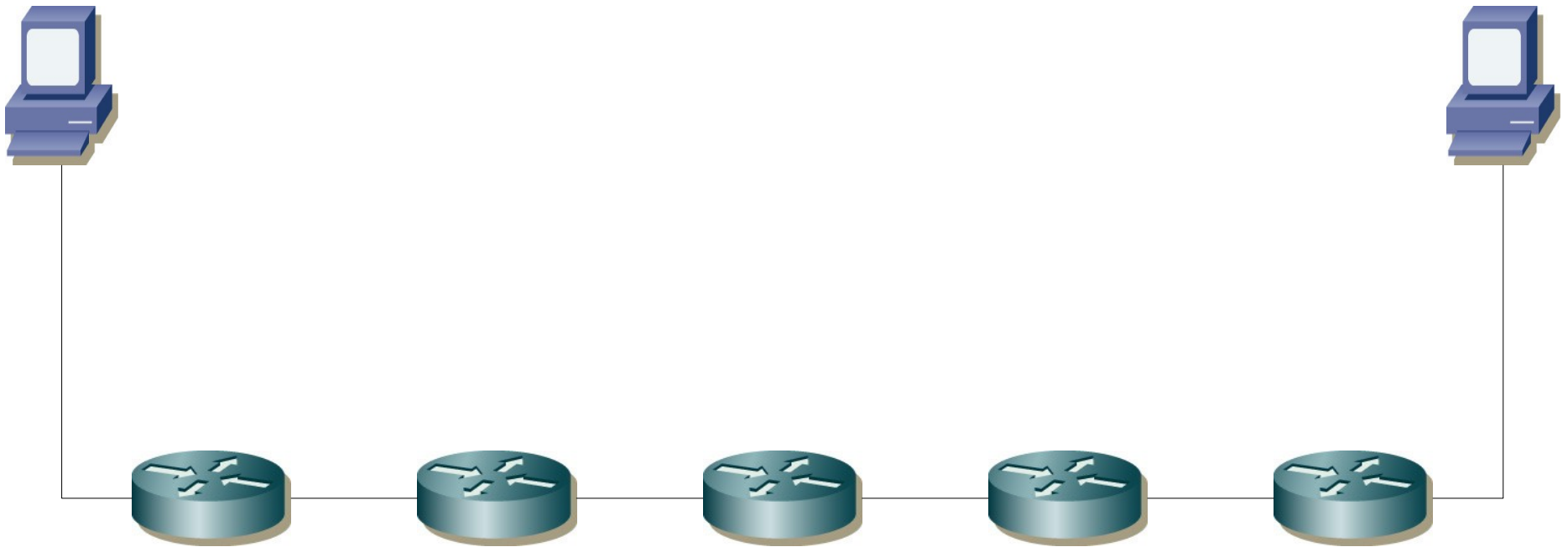
Introducción

- Envío de paquetes con TTL incremental.
- V. Jacobson (1989).
- Traceroute comúnmente usa UDP y ICMP.
- Recepción de cada nodo intermedio de paquete de error ICMP TTL EXCEEDED.
- Del equipo destino paquete ECHO REPLY o UDP PORT UNREACHABLE.

Introducción

Origen

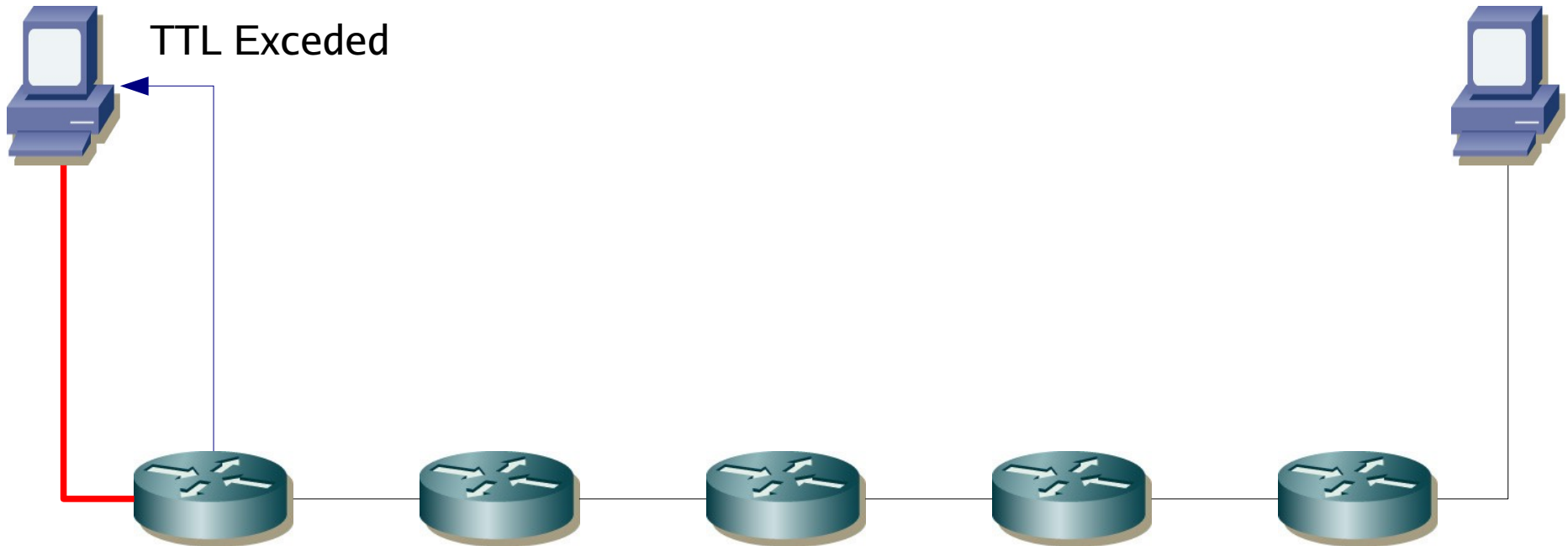
Destino



Introducción

Origen

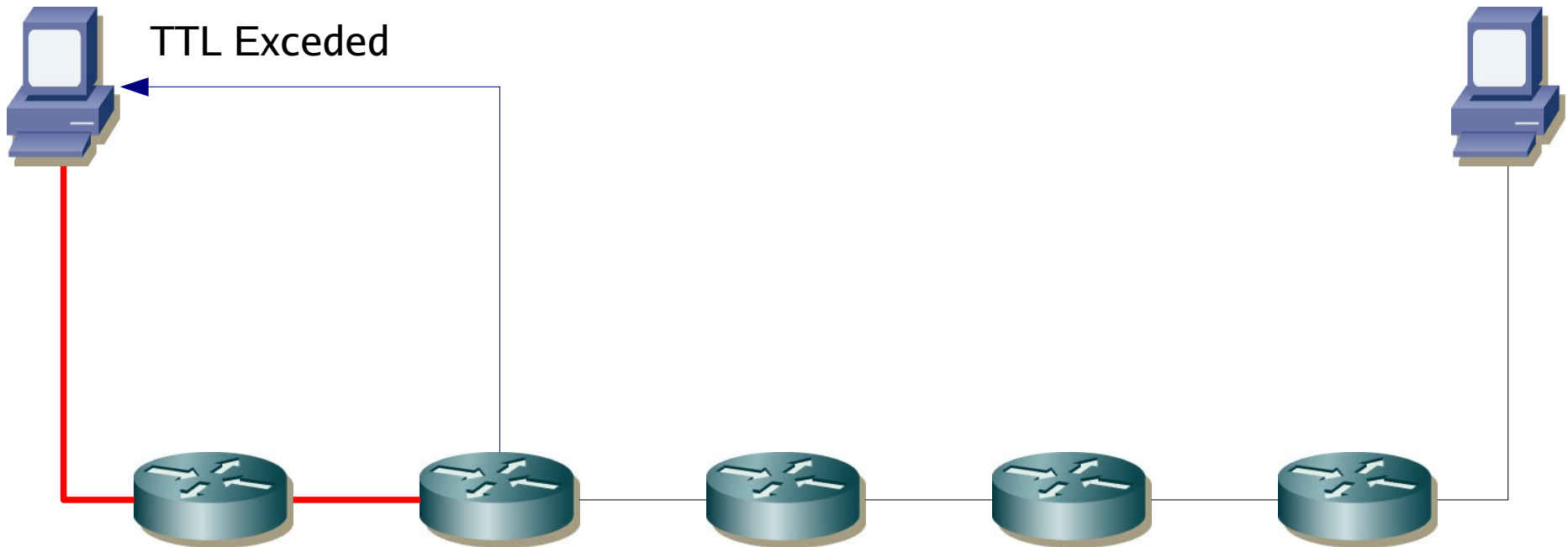
Destino



Introducción

Origen

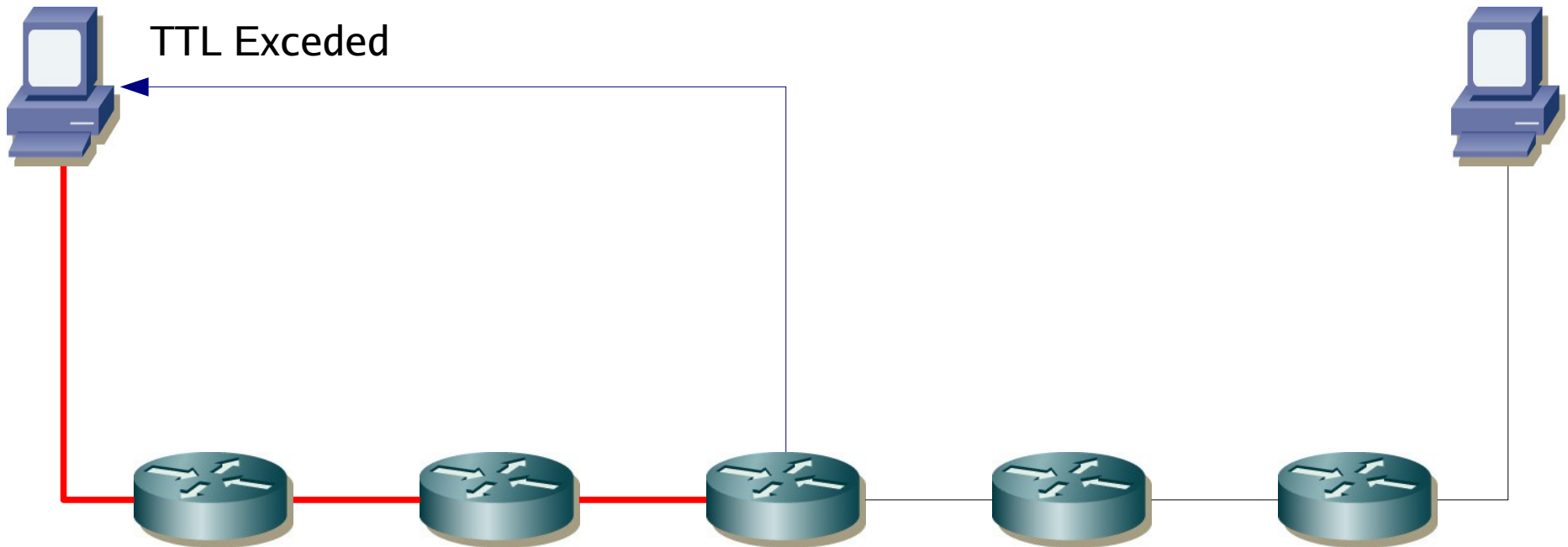
Destino



Introducción

Origen

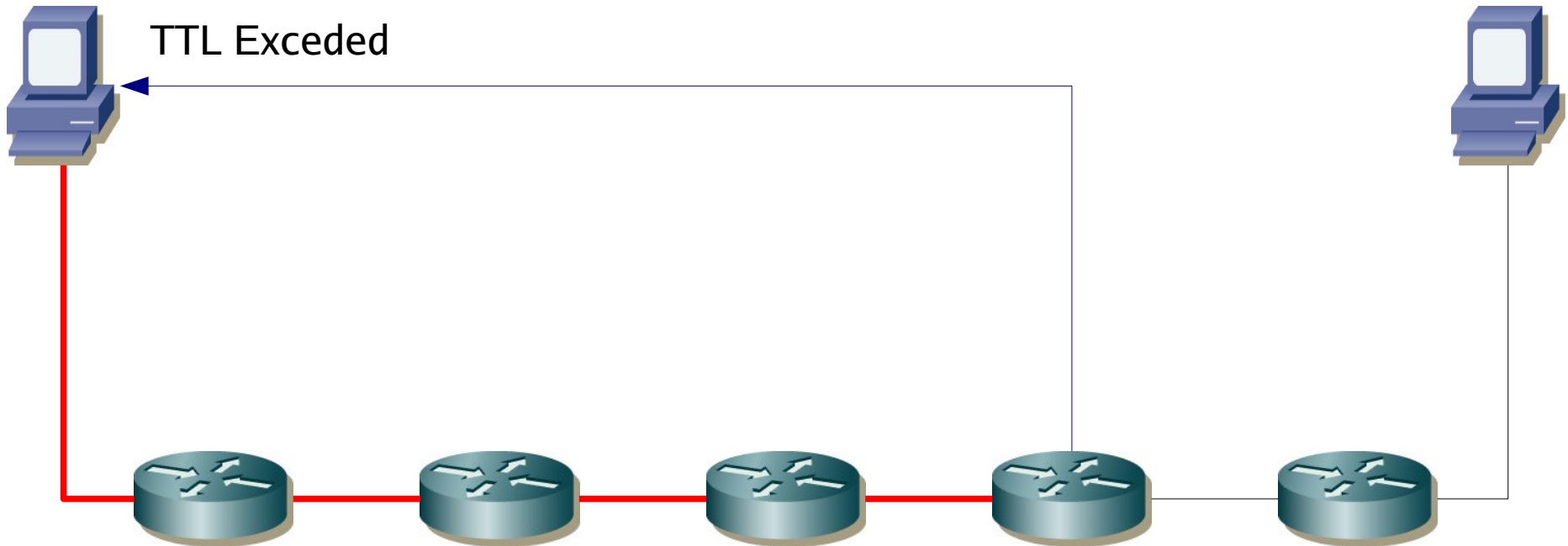
Destino



Introducción

Origen

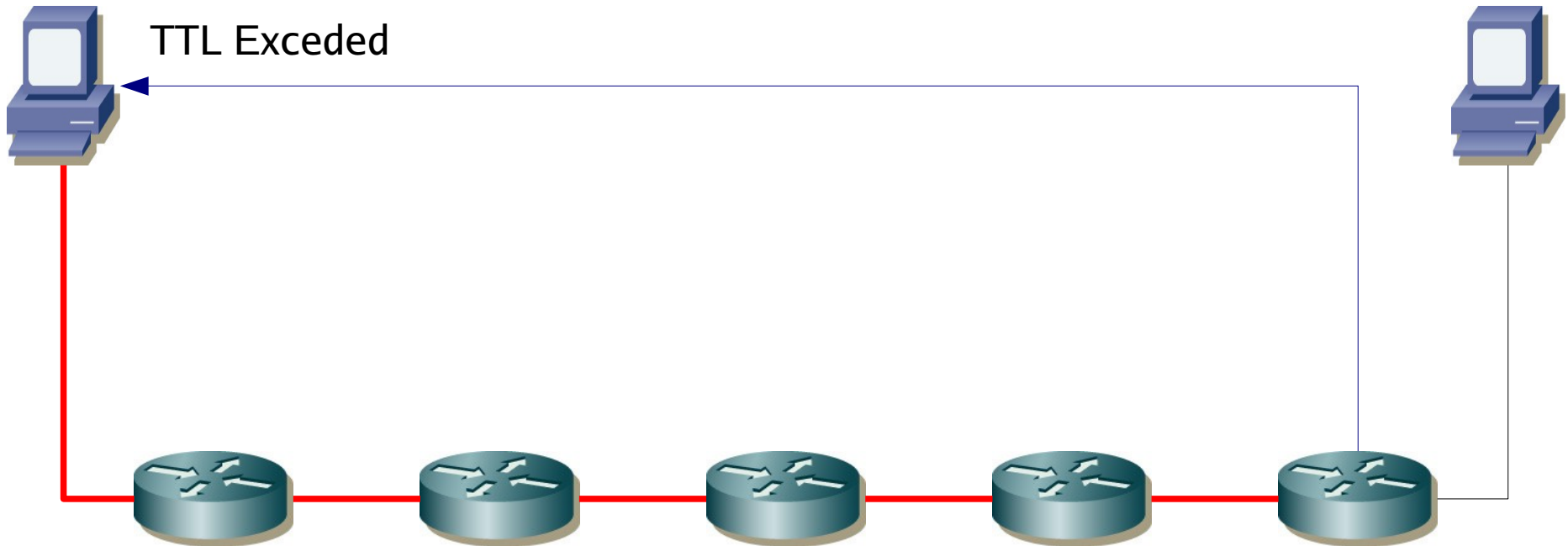
Destino



Introducción

Origen

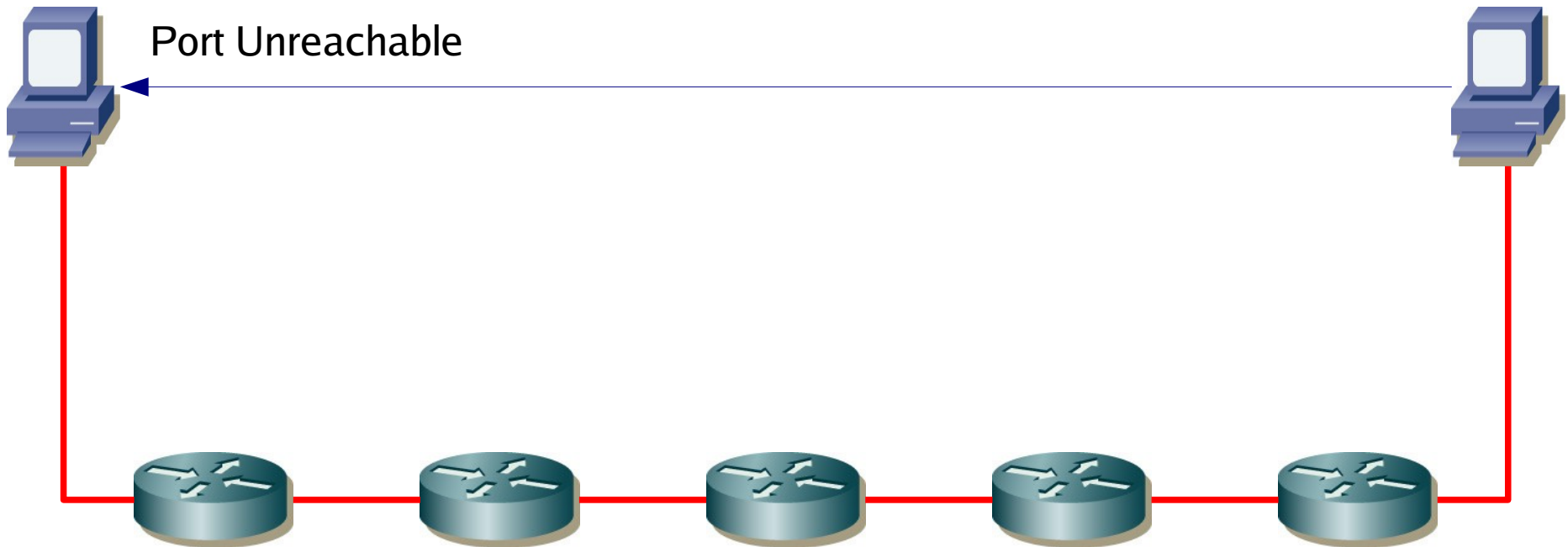
Destino



Introducción

Origen

Destino



Índice

- Introducción
- Problemas
- Soluciones
- Implementación
- Pruebas

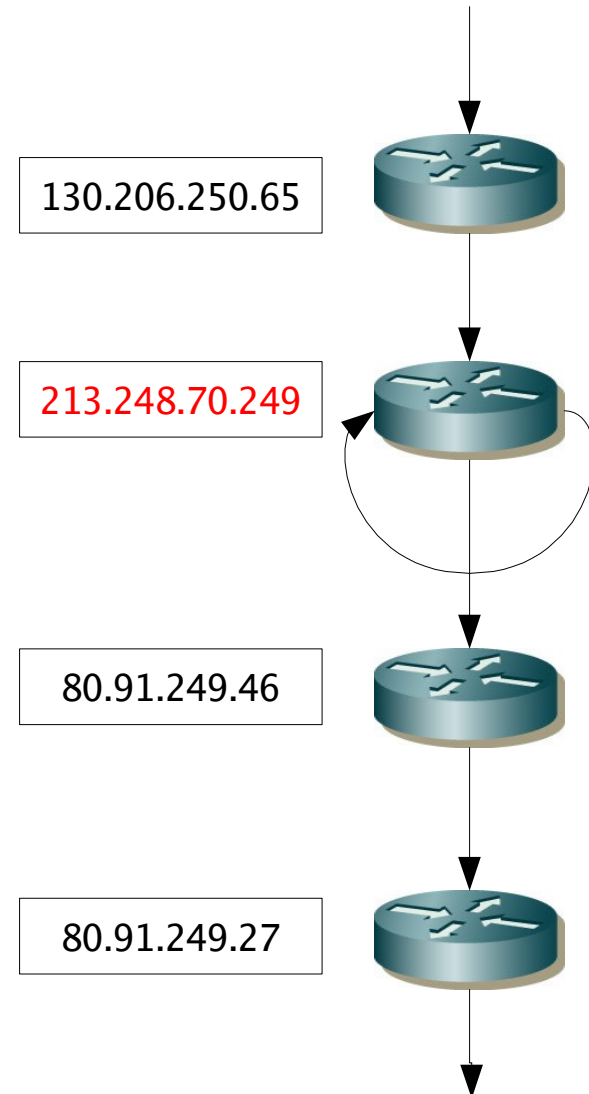
Problemas

- Ver enlaces que realmente no existen:
 - Ciclos
 - Diamantes

Problemas

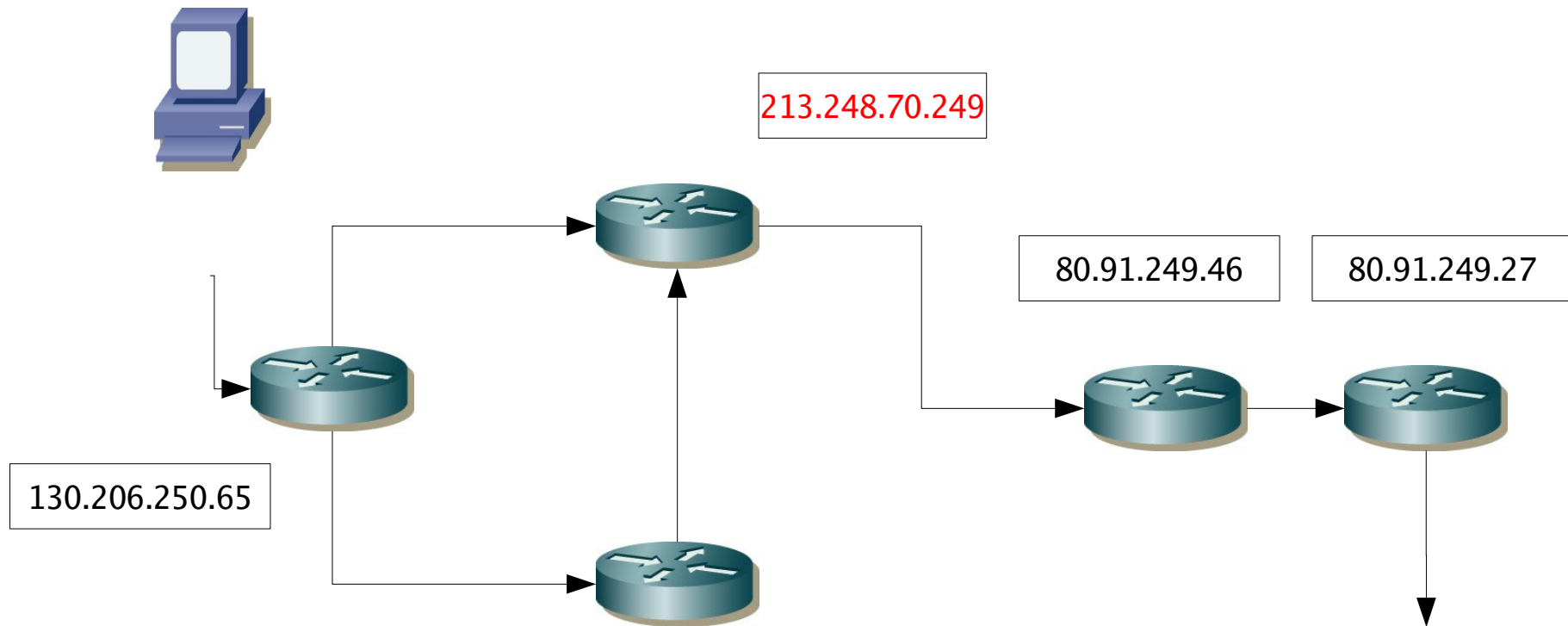
- Ciclos

1	130.206.160.1	0.344 ms	0.286 ms	0.317 ms
2	130.206.158.17	0.367 ms	0.515 ms	0.213 ms
3	130.206.158.1	1.275 ms	1.128 ms	1.178 ms
4	130.206.209.13	1.699 ms	1.976 ms	1.770 ms
5	130.206.250.121	8.793 ms	8.693 ms	46.958 ms
6	130.206.250.65	41.138 ms	20.281 ms	20.109 ms
7	213.248.70.249	24.743 ms	19.804 ms	20.347 ms
8	213.248.70.249	47.782 ms	213.4.70.2	46.682 ms 47.496 ms
9	80.91.249.46	57.088 ms	56.915 ms	56.841 ms
10	80.91.249.27	69.587 ms	69.809 ms	69.858 ms
11	213.248.76.2	70.842 ms	70.604 ms	71.080 ms
12	195.3.70.189	70.943 ms	70.760 ms	195.3.70.89 71.124 ms
13	195.3.70.38	69.967 ms	70.005 ms	69.684 ms



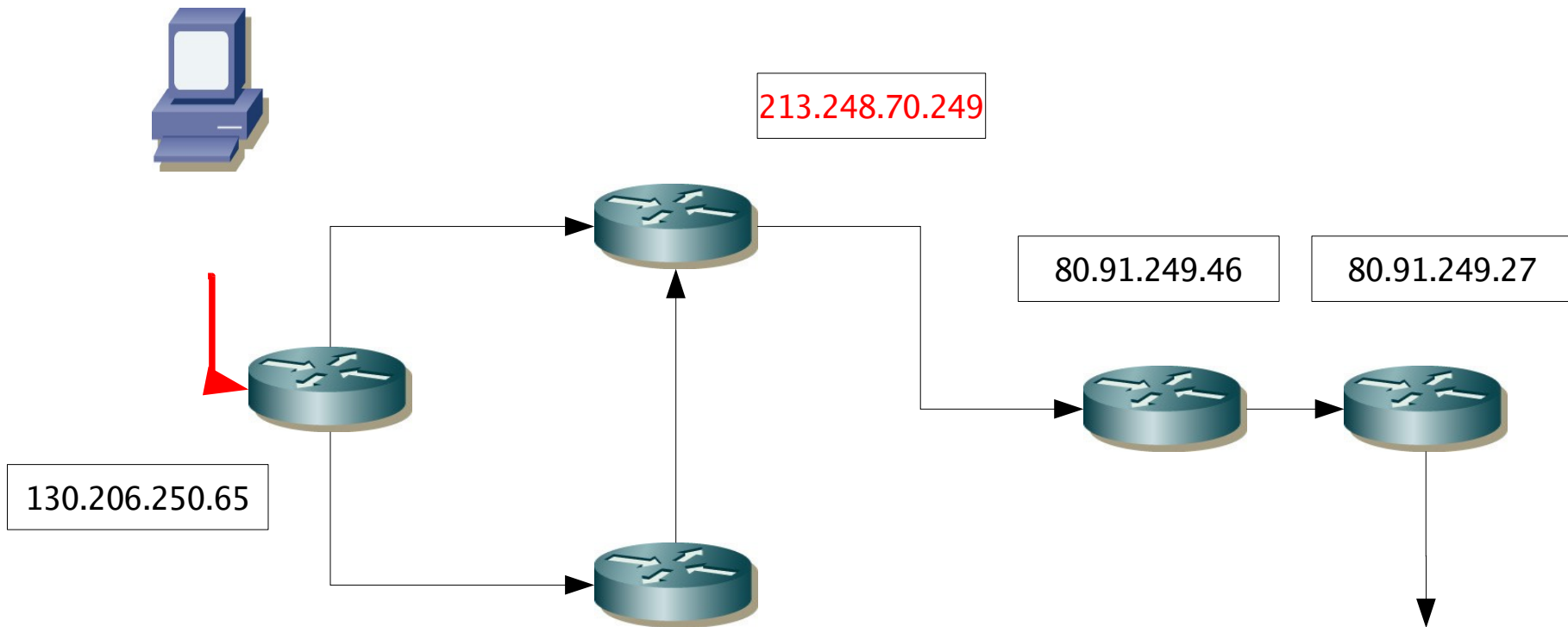
Problemas

- Ciclos(Motivo 1)



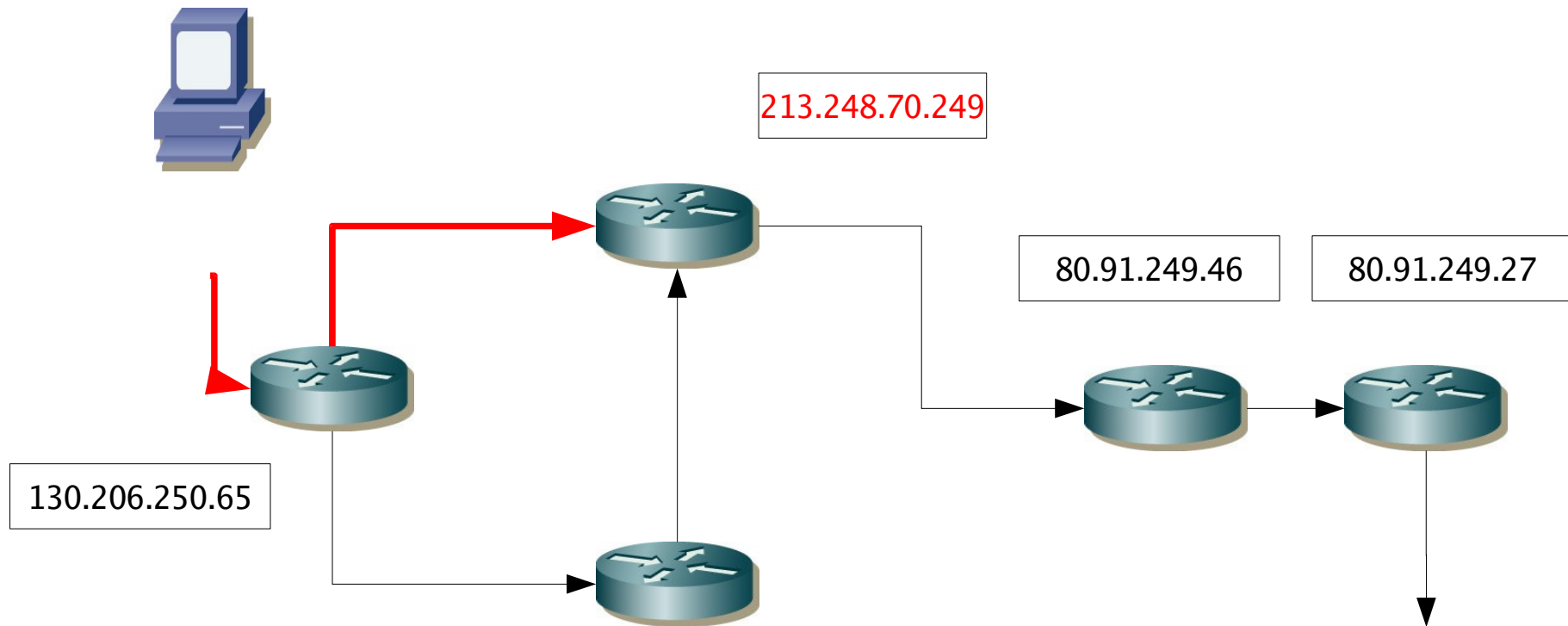
Problemas

- Ciclos(Motivo 1)



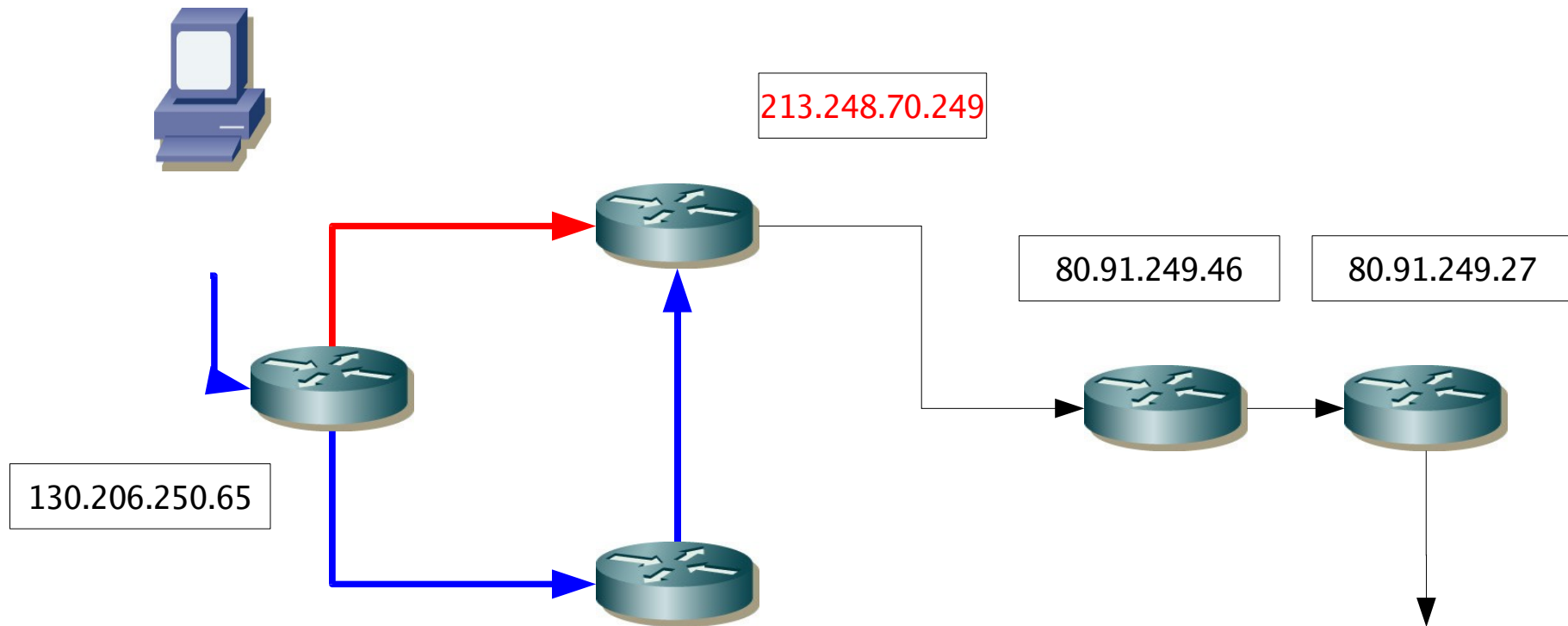
Problemas

- Ciclos(Motivo 1)



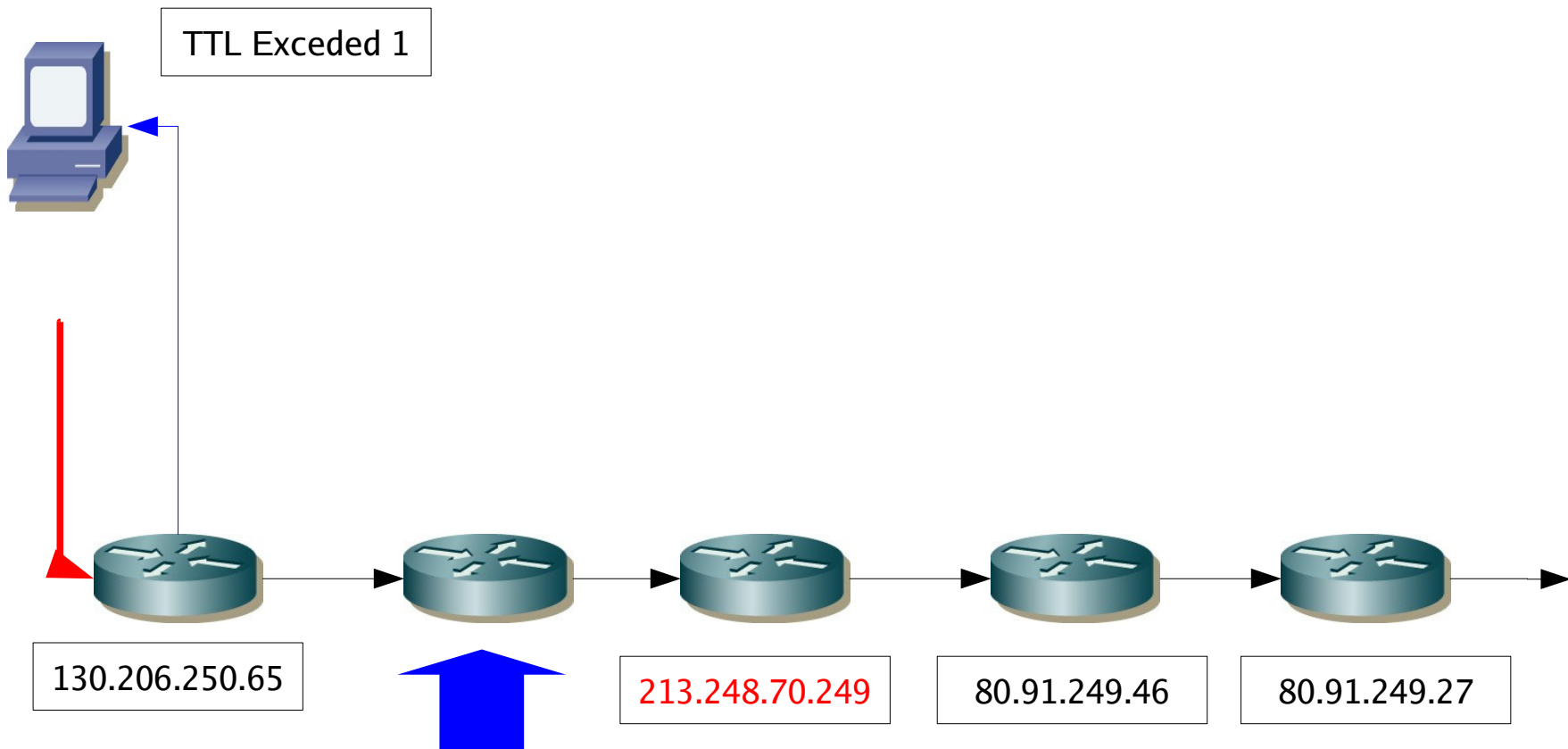
Problemas

- Ciclos(Motivo 1)



Problemas

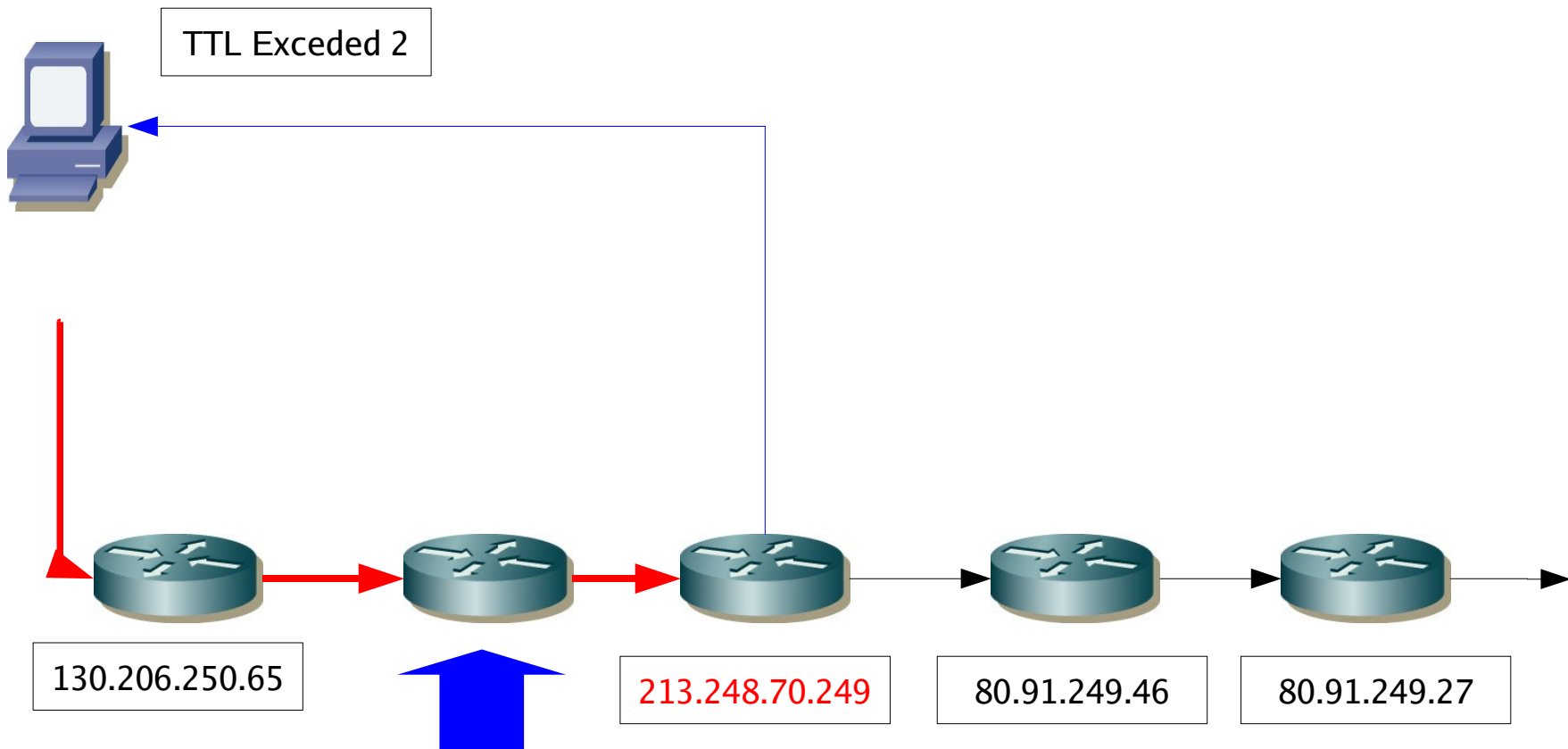
- Ciclos(Motivo 2)



Mala configuración, reenvía
paquetes con TTL = 0

Problemas

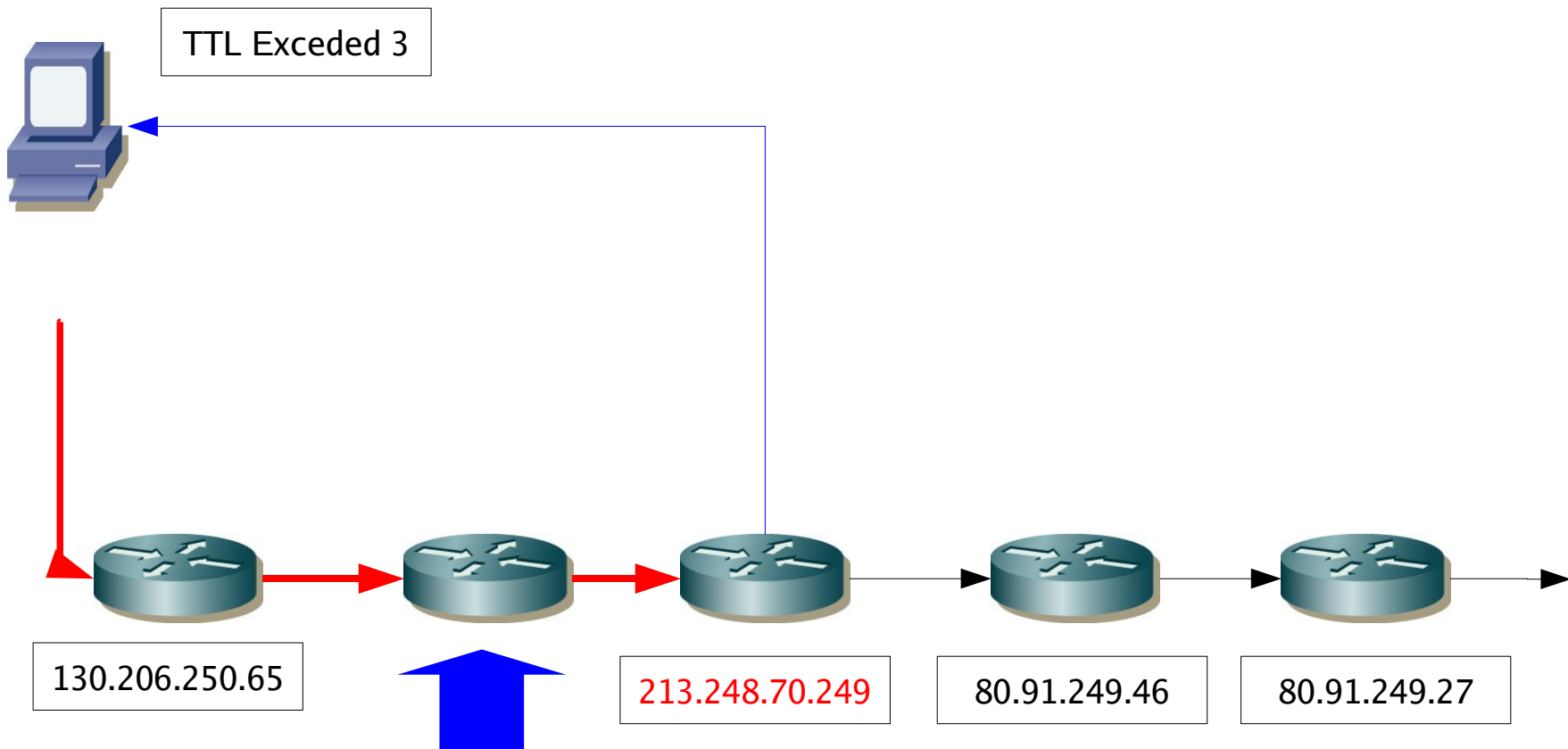
- Ciclos(Motivo 2)



Mala configuración, reenvía
paquetes con TTL = 0

Problemas

- Ciclos(Motivo 2)

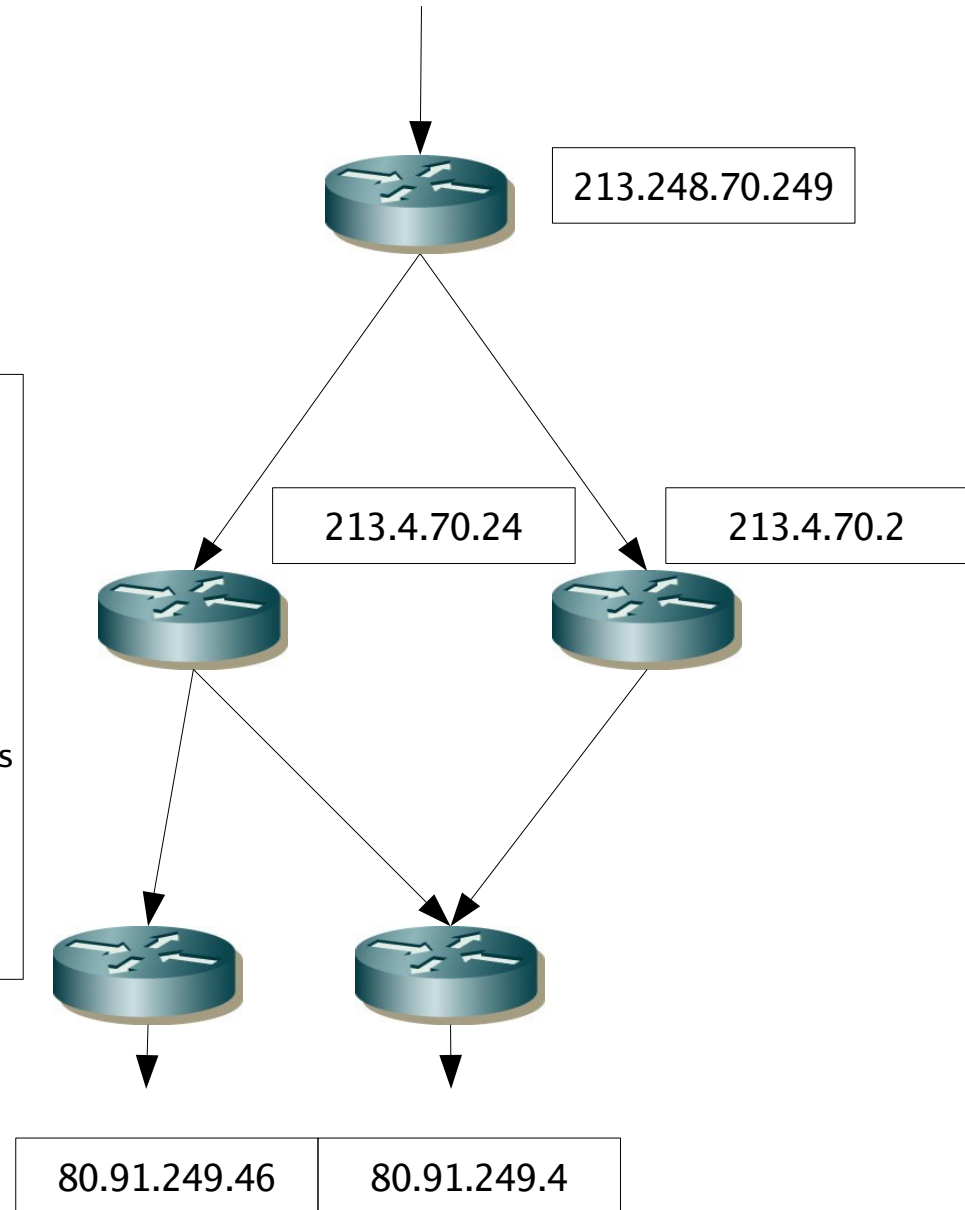


Mala configuración, reenvía
paquetes con TTL = 0

Problemas

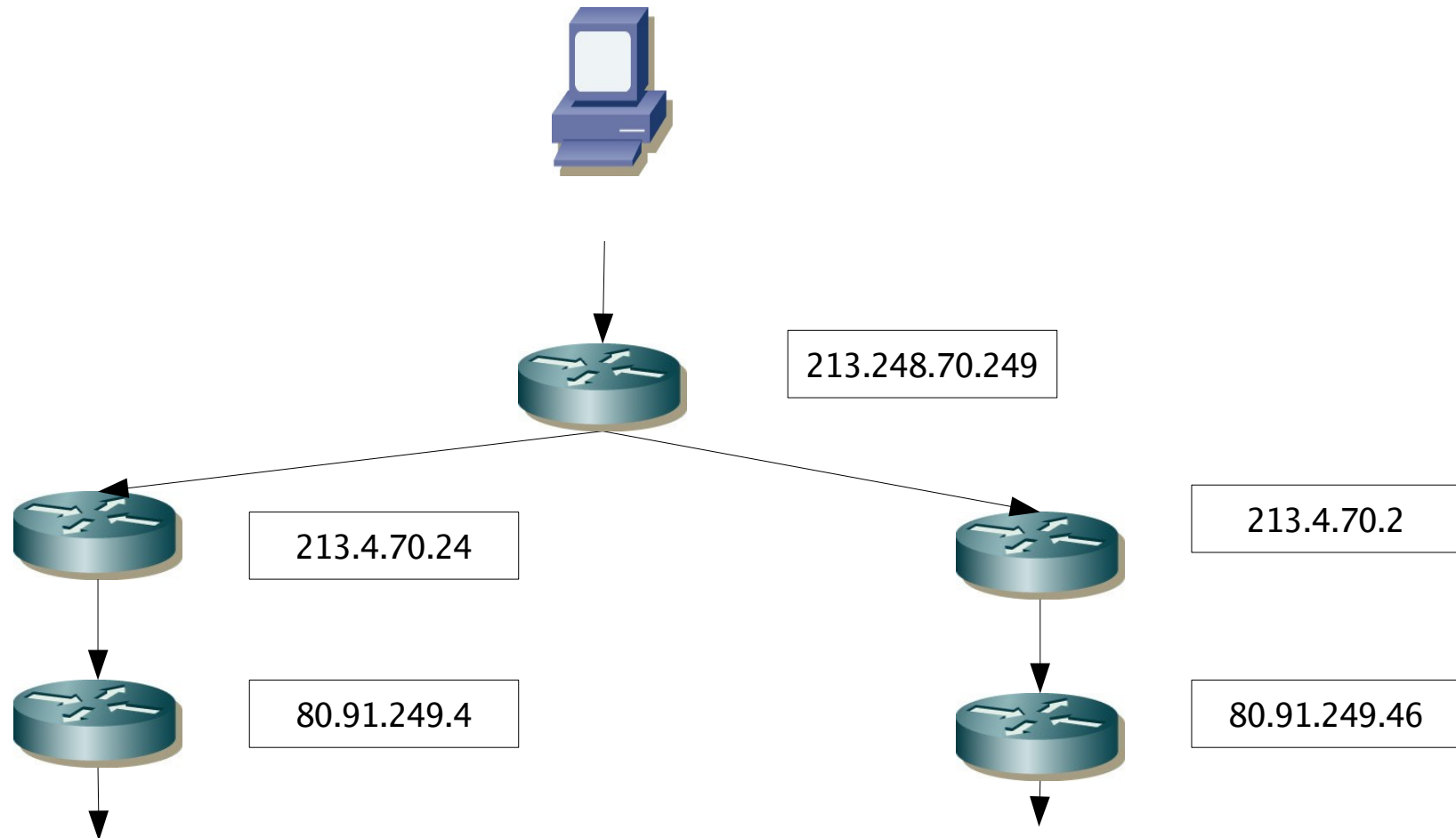
- Diamantes

1	130.206.160.1	0.344 ms	0.286 ms	0.317 ms		
2	130.206.158.17	0.367 ms	0.515 ms	0.213 ms		
3	130.206.158.1	1.275 ms	1.128 ms	1.178 ms		
4	130.206.209.13	1.699 ms	1.976 ms	1.770 ms		
5	130.206.250.121	8.793 ms	8.693 ms	46.958 ms		
6	130.206.250.65	41.138 ms	20.281 ms	20.109 ms		
7	213.248.70.249	24.743 ms	19.804 ms	20.347 ms		
8	213.4.70.24	47.782 ms	213.4.70.2	46.682 ms	213.4.70.24	47.496 ms
9	80.91.249.46	57.088 ms	80.91.249.4	56.915 ms	80.91.249.4	56.841 ms
10	80.91.249.27	69.587 ms	69.809 ms	69.858 ms		
11	213.248.76.2	70.842 ms	70.604 ms	71.080 ms		
12	195.3.70.189	70.943 ms	70.760 ms	195.3.70.89	71.124 ms	
13	195.3.70.38	69.967 ms	70.005 ms	69.684 ms		



Problemas

- Diamantes(Motivo)



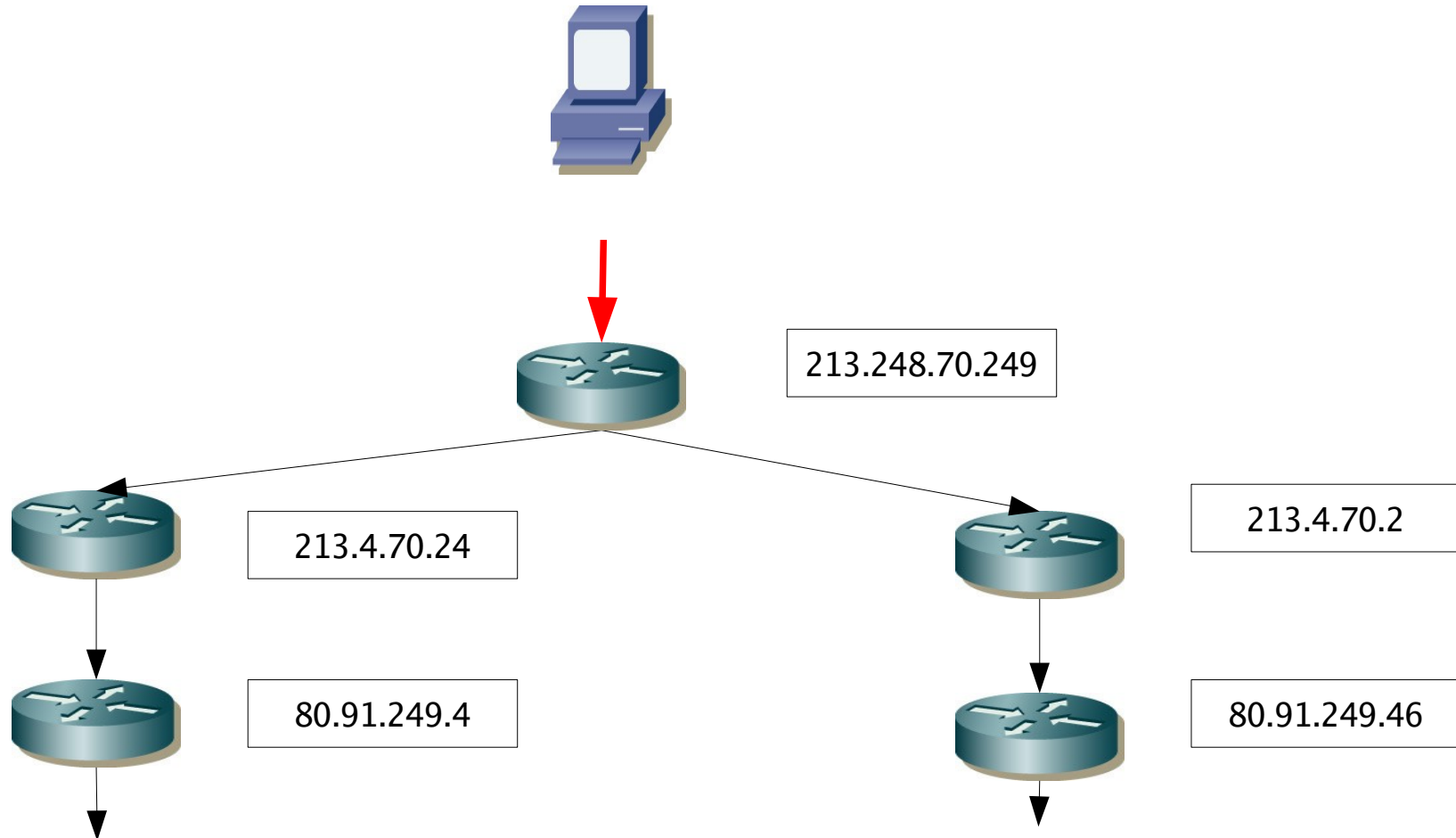
Problemas

213.248.70.249

213.248.70.249

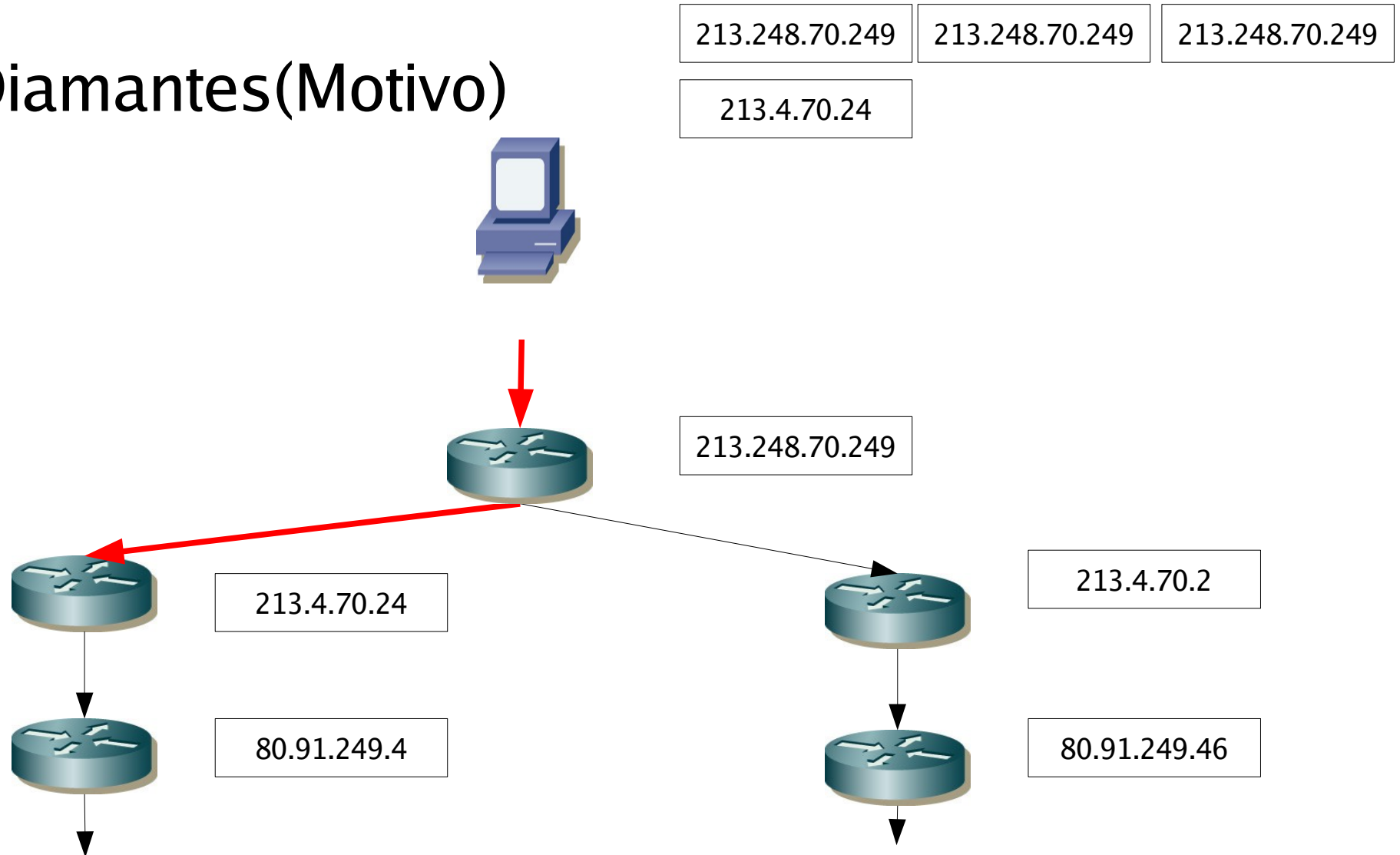
213.248.70.249

- Diamantes(Motivo)



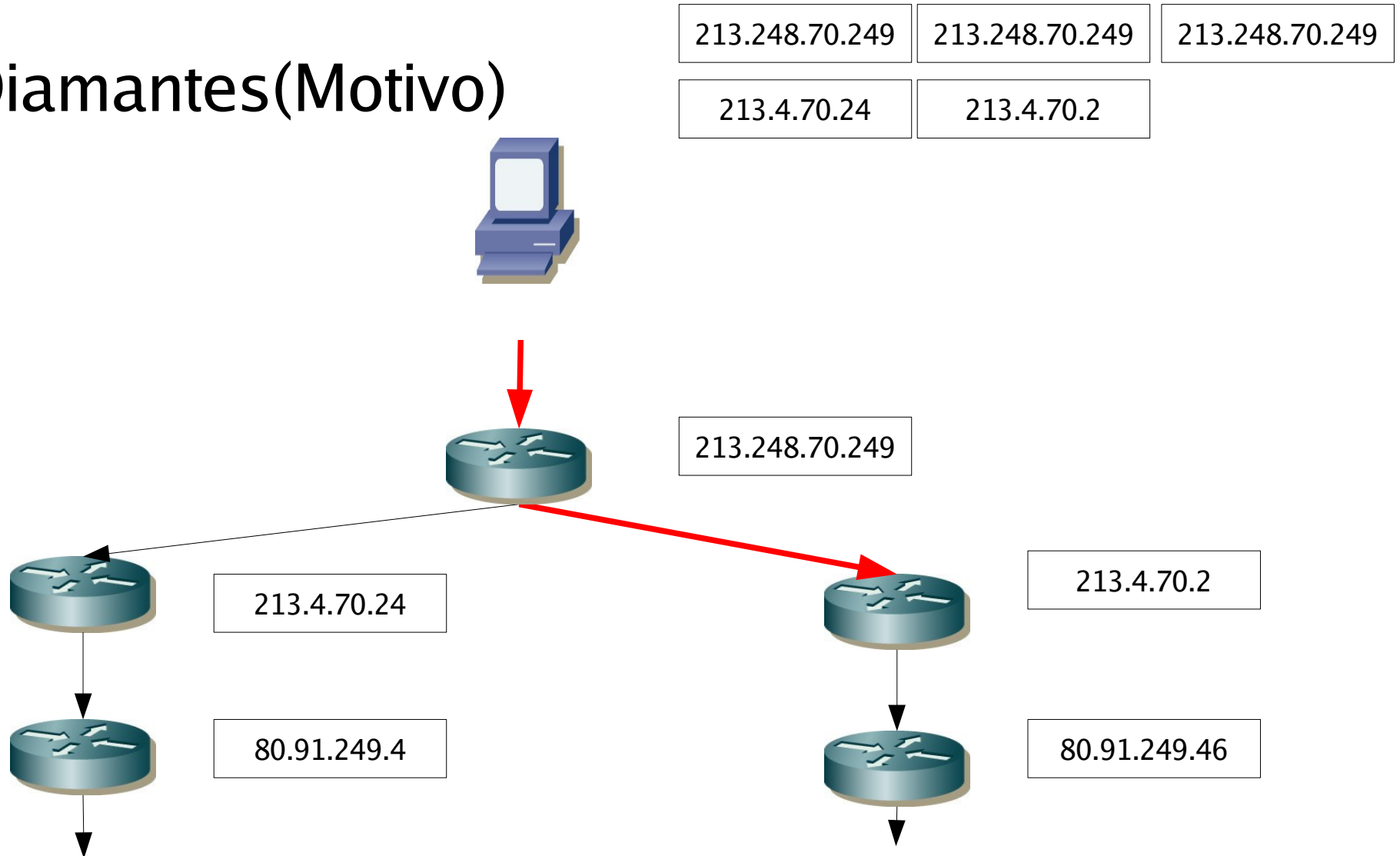
Problemas

- Diamantes(Motivo)



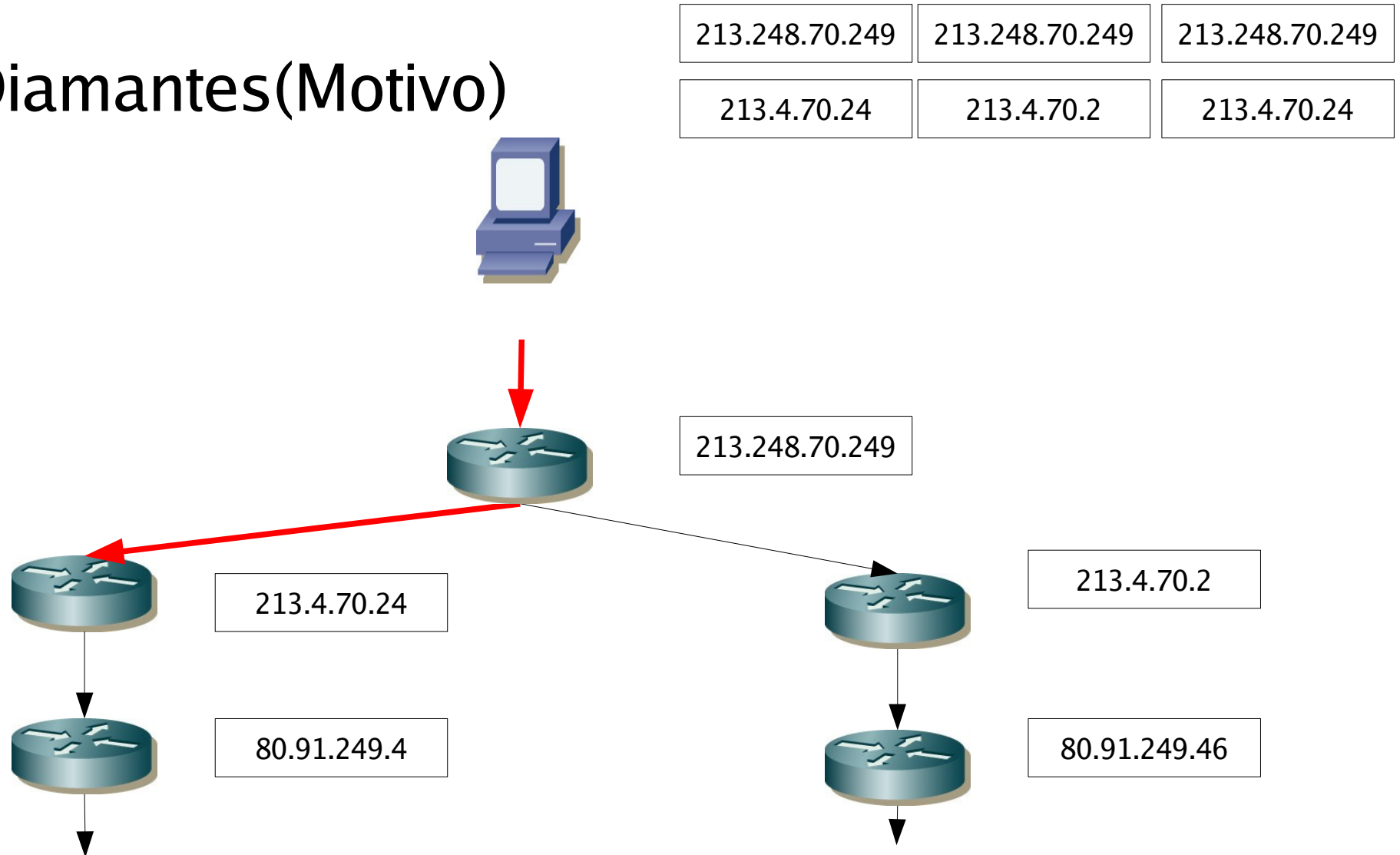
Problemas

- Diamantes(Motivo)



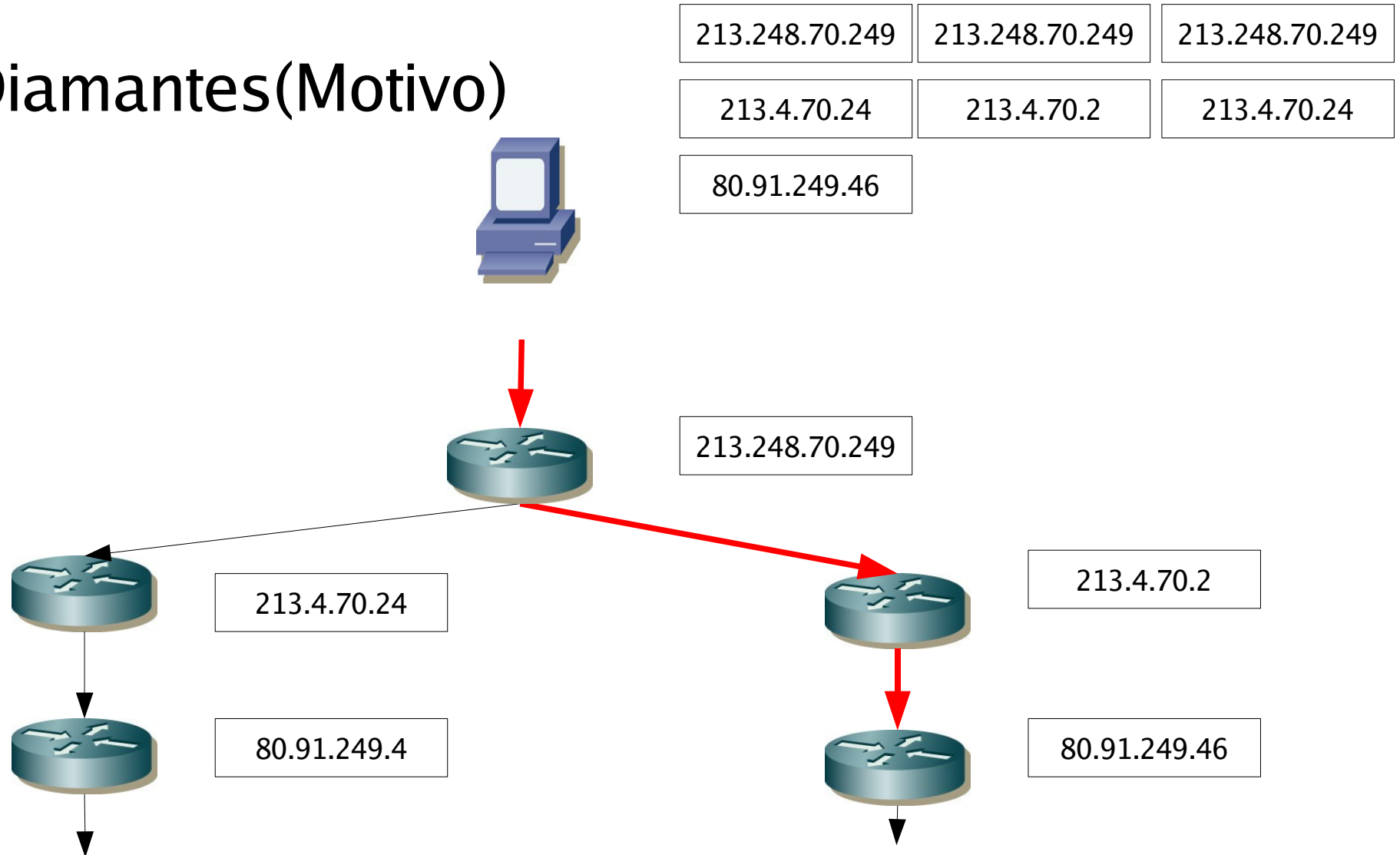
Problemas

- Diamantes(Motivo)



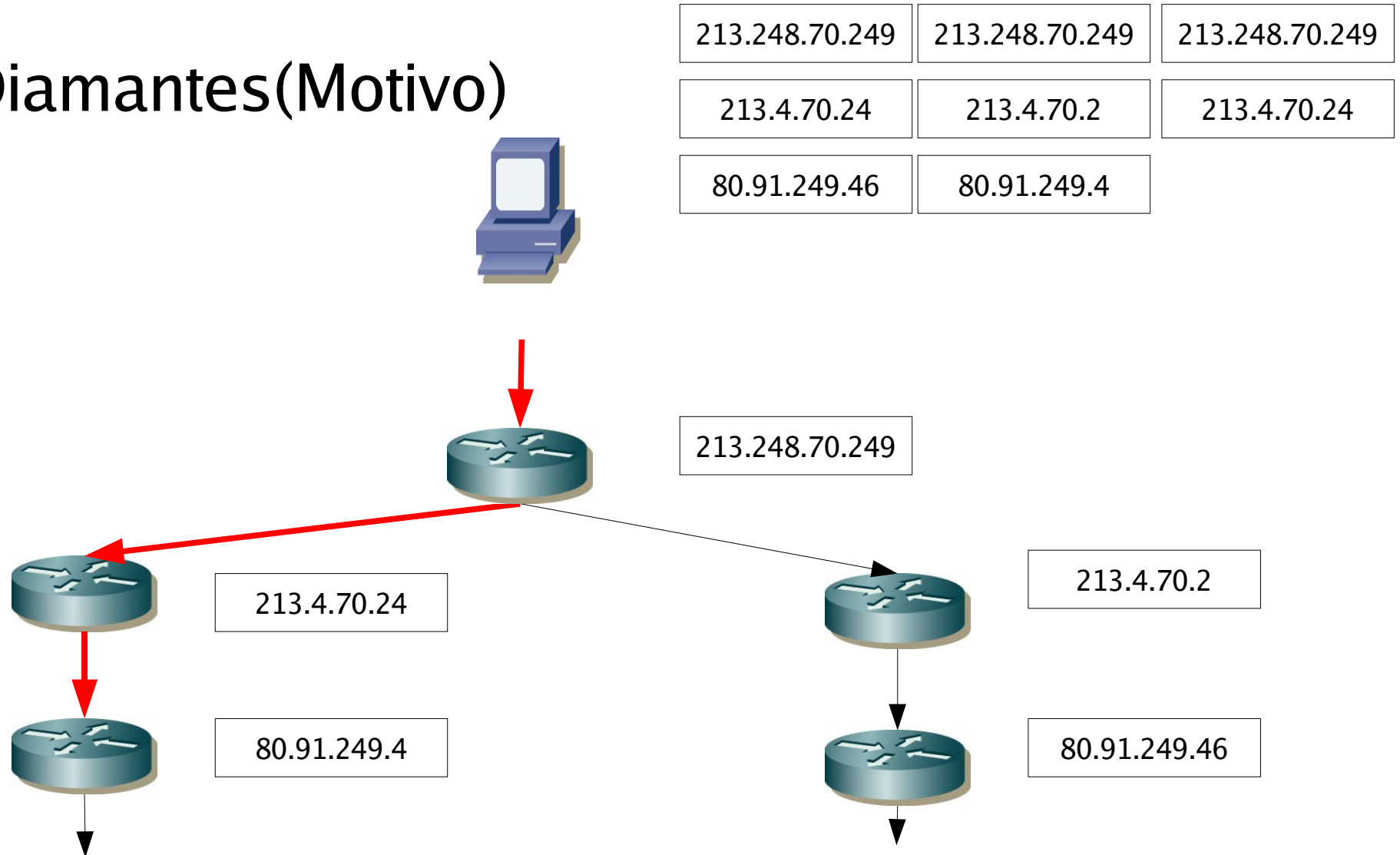
Problemas

- Diamantes(Motivo)



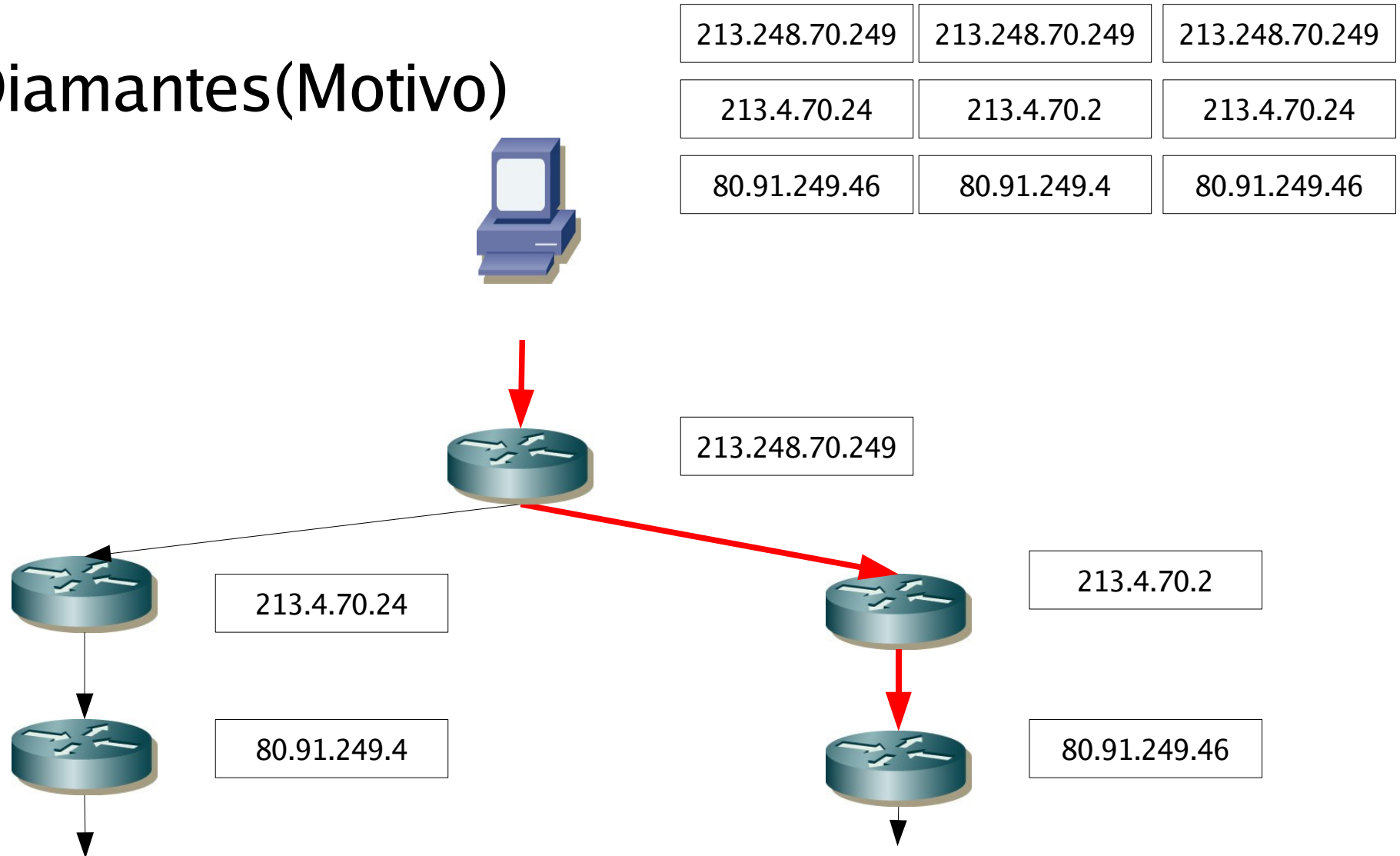
Problemas

- Diamantes(Motivo)



Problemas

- Diamantes(Motivo)

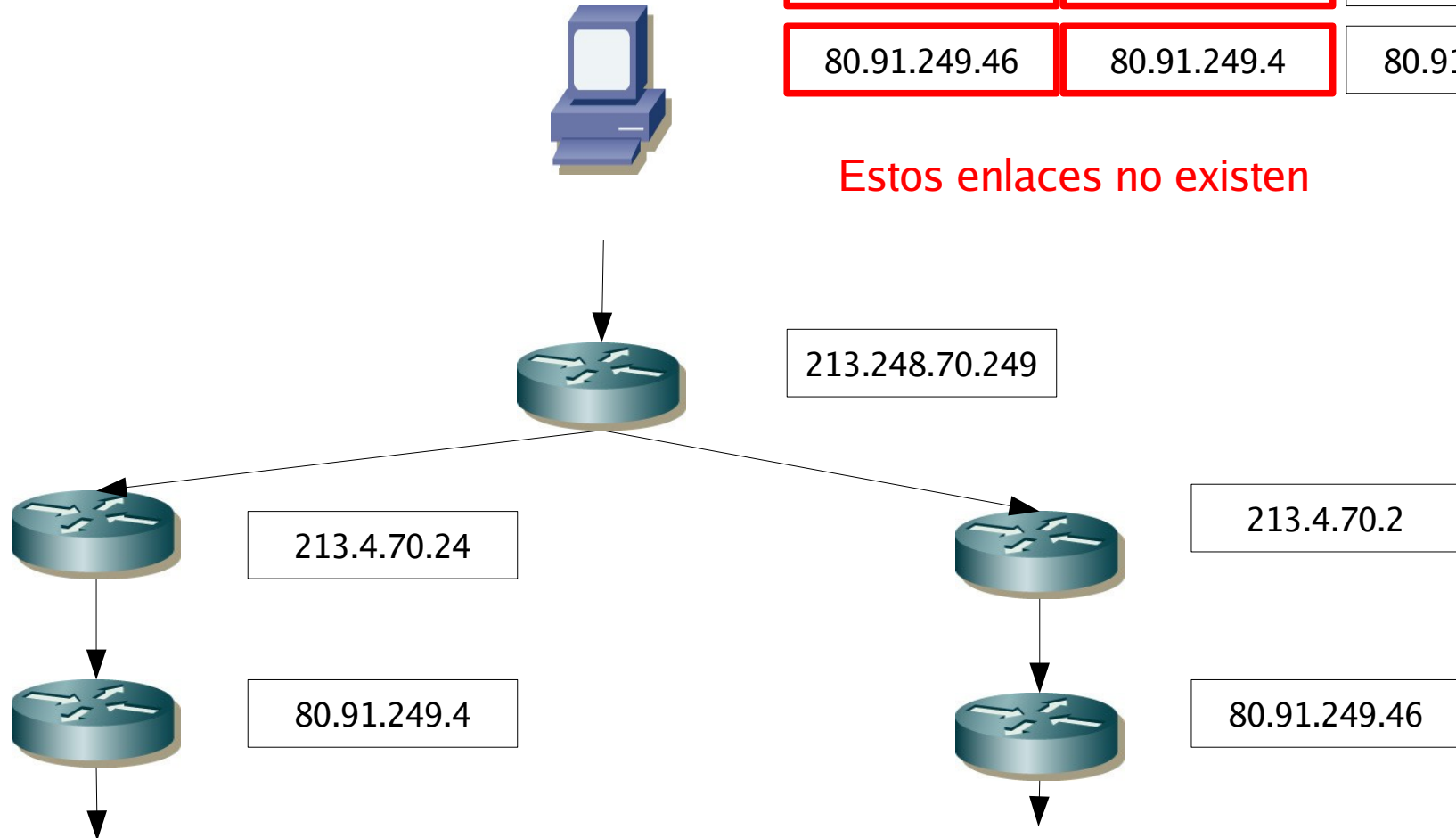


Problemas

- Diamantes(Motivo)

213.248.70.249	213.248.70.249	213.248.70.249
213.4.70.24	213.4.70.2	213.4.70.24
80.91.249.46	80.91.249.4	80.91.249.46

Estos enlaces no existen



Índice

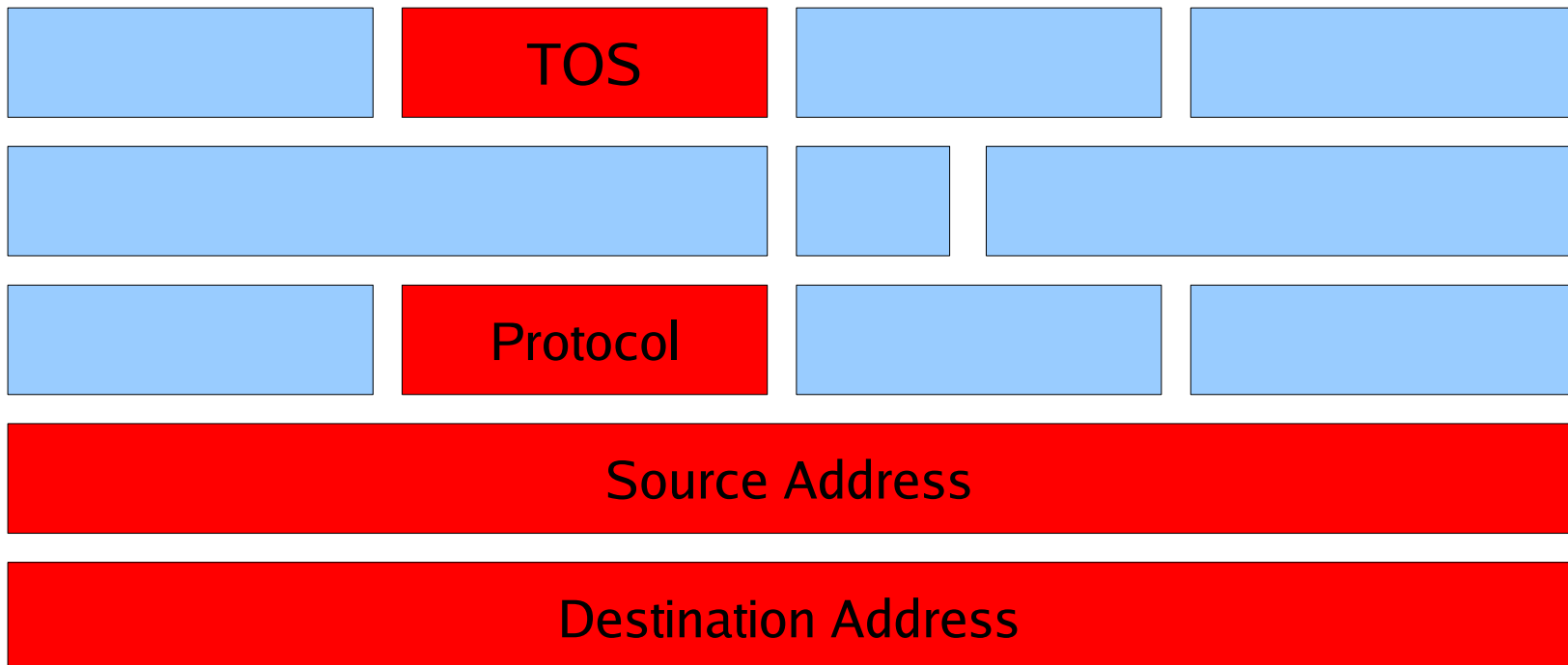
- Introducción
- Problemas
- Soluciones
- Implementación
- Pruebas

Soluciones

- Paris traceroute Brice Augustin (2006)
- Plantean que generalmente el balanceo de carga se hace por flujo.
- Basándose en pruebas realizadas con TCP, UDP e IPsec ven que el balanceo se hace ciegamente usando los 4 primeros octetos de la capa transporte.

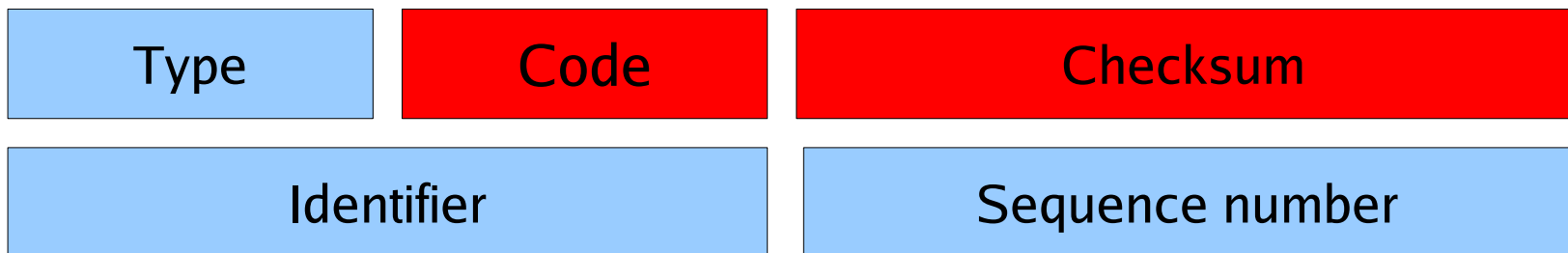
Soluciones

- Mantener ciertos campos para preservar el flujo y que no haya balanceo:
- IP



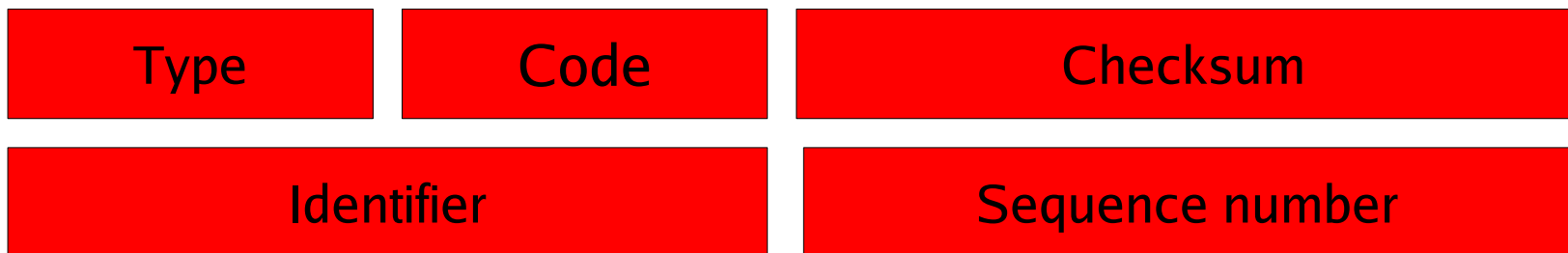
Soluciones

- Mantener ciertos campos para preservar el flujo y que no haya balanceo:
- ICMP



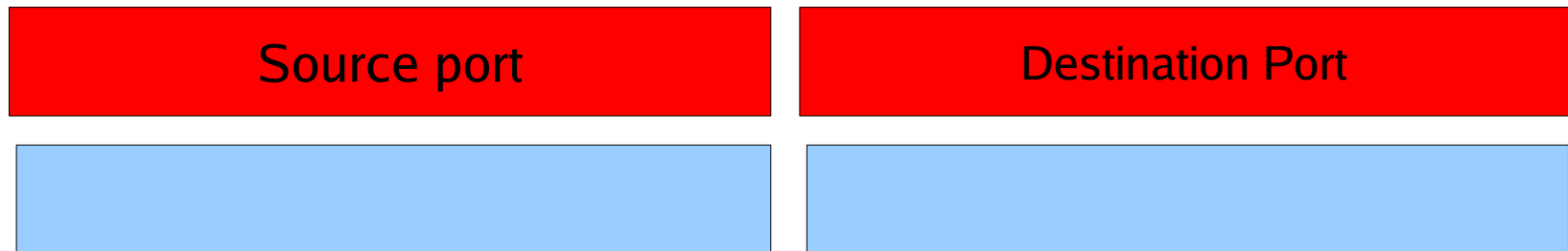
Soluciones

- Mantener ciertos campos para preservar el flujo y que no haya balanceo:
- ICMP
- Debido al checksum



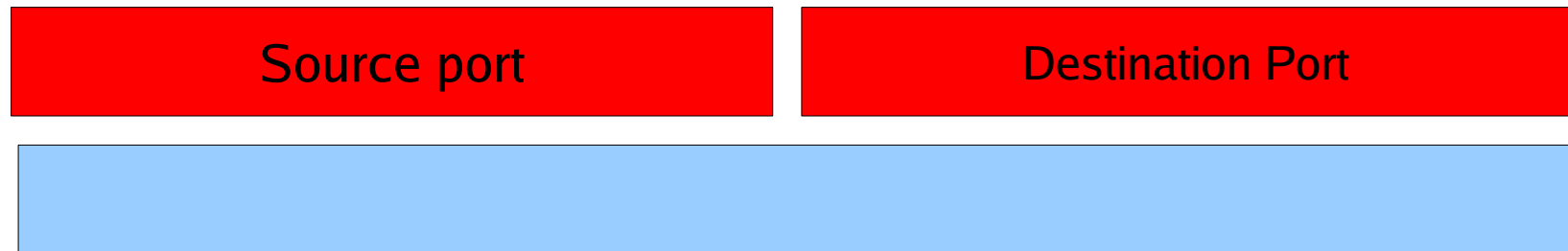
Soluciones

- Mantener ciertos campos para preservar el flujo y que no haya balanceo:
- UDP



Soluciones

- Mantener ciertos campos para preservar el flujo y que no haya balanceo:
- TCP



Índice

- Introducción
- Problemas
- Soluciones
- Implementación
- Pruebas

Implementación

- Se han programado 4 programas:
 - Newtraceroute
 - Newtracerouteparisicmp
 - Newtracerouteparisudp
 - Newtracerouteparistcp
- Usando librerías:
 - Libpcap
 - Libnet
 - inet

Implementación

- Salida de los programas:

```
1 192.71.20.97 777 11 0 255 8D28
1 192.71.20.97 721 11 0 255 8D29
1 192.71.20.97 809 11 0 255 8D2A
2 192.71.20.10 778 11 0 254 E9A2
2 192.71.20.10 835 11 0 254 E9A3
2 192.71.20.10 730 11 0 254 E9A4
```

stdout

```
45 00 00 26 6F 8F 00 00 2E 01
21 F7 82 CE A3 A5 C0 47 14 96
00 00 75 5A 00 00 00 00 52 65
73 65 61 72 63 68 00 00
E & o .
!?? ?G
uZ Re
search
```

stderr

Índice

- Introducción
- Problemas
- Soluciones
- Implementación
- Pruebas

Pruebas

- Para todos los nodos de ETOMIC con todos los demás:
 - Varios test consistentes en:
 - 30 Pruebas con 3 peticiones por TTL
 - Para ver si se consiguen descubrir los diversos caminos con Paris traceroute.
 - 1 Prueba con 30 peticiones por TTL
 - Para ver si realmente no sufre de balanceo o si hay algún router con balanceo por paquete

Pruebas

- No se detectó después de la depuración de programas ningún balanceo en las pruebas de Paris Traceroute.
- Se detecto que si se descubrían los distintos caminos con pruebas sucesivas.

Pruebas

