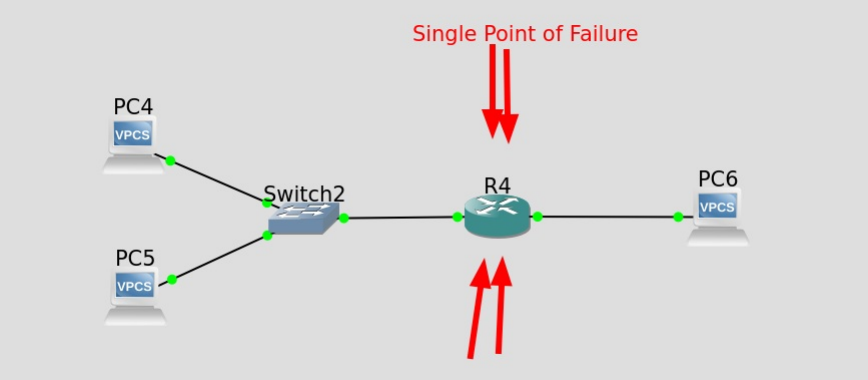
Single Point of Failure



- Neste exemplo temos um SPOF(Single Point of Failure). Conseguimos perceber que se o R4 deixar de funcionar deixa de haver ligação entre a rede da esquerda e a rede da direita.
- Sendo assim o primeiro passo para eliminar este SPOF é utilizar outro router
- Depois disto temos de conjugar a rede de modo a termos um *down time* pequeno pois o conseguimos eliminar de todo
- E temos tambem de utilizar estratégias para que caso haja um SPOF o router de backup consiga fazer o mesmo trabalho do router original
- Em baixo estão algumas estratégias para tolerar falhas no *default gateway*

2 Routers - 2 DHCP Servers

Configurando o DHCP Server no R1

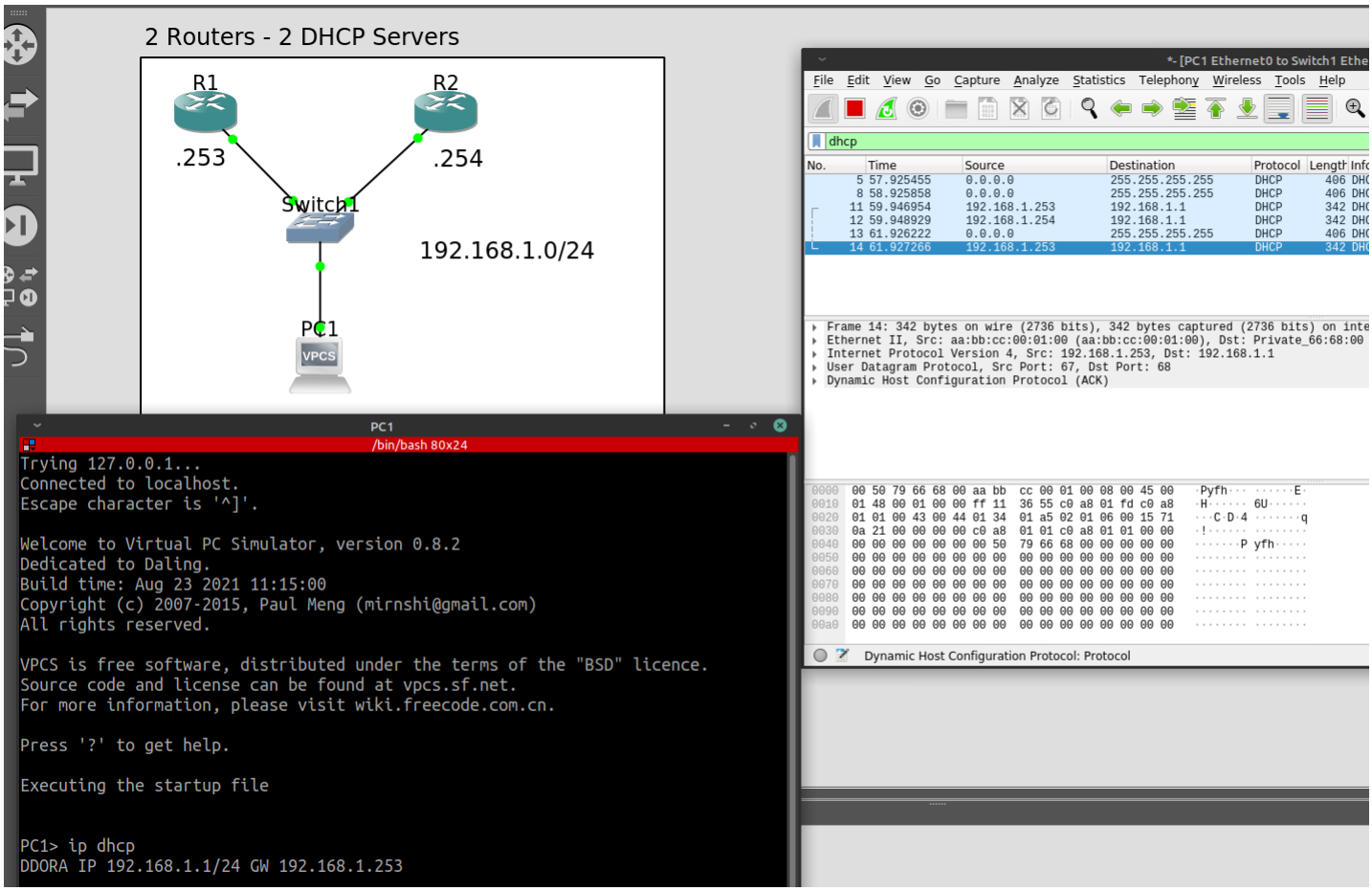
```
conf t
ip dhcp pool R1POOL
network 192.168.1.0 255.255.255.0
default-router 192.168.1.253
exit
ip dhcp excluded-address 192.168.1.253 192.168.1.254
```

Configurando o DHCP Server no R2

```
conf t
ip dhcp pool R2POOL
network 192.168.1.0 255.255.255.0
default-router 192.168.1.254
exit
ip dhcp excluded-address 192.168.1.253 192.168.1.254
```

O que acontece se o PC1 pedir um IP ?

- O PC1 envia um DHCP Discover em broadcast para ver se existe algum servidor DHCP disponivel
- Ambos os routers escutam esse pedido e respondem com um DHCP Offer
- Depois disto o PC1 vai aceitar de maneira aleatória a oferta do R1 ou do R2 fazendo um DHCP Request
- Por fim, o router escolhido pelo PC1 vai enviar o IP ao PC1 com o DHCP Ack
- Ou seja, esta comunicação é sempre feita em broadcast até o router enviar o IP na ultima comunicação



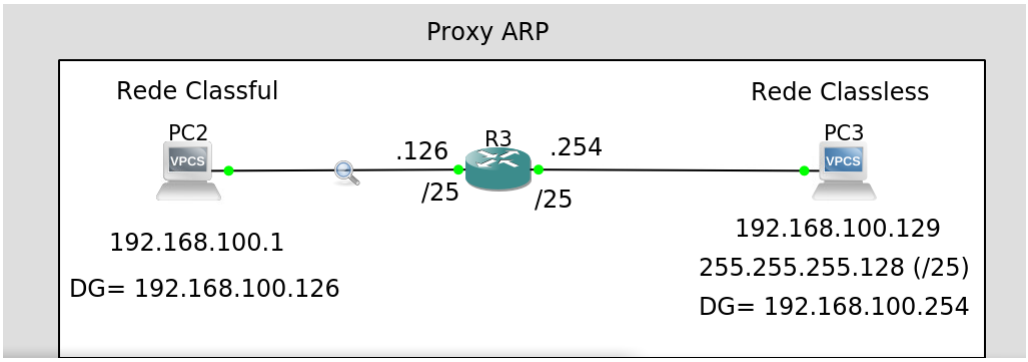
Proxy ARP

Atenção que o proxy arp vem ativado por omissão

PC 1 -> `ip 192.168.100.1 255.255.255.0 192.168.100.126` PC2 -> `ip 192.168.100.129 255.255.128 192.168.100.254`

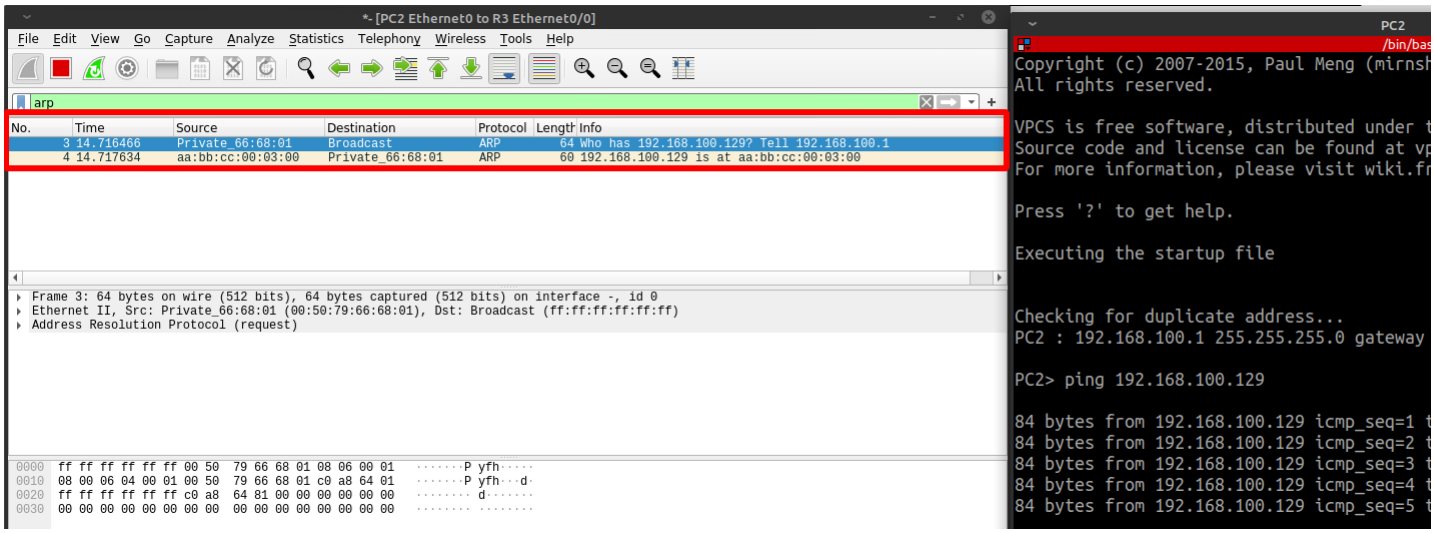
R1 (e0/0) -> `ip add 192.168.100.126 255.255.255.128` R1 (e0/1) -> `ip add 192.168.100.254 255.255.255.128`

Ativar o proxy arp -> `int e0/0 ; ip proxy-arp`



O que é que acontece nesta situação?

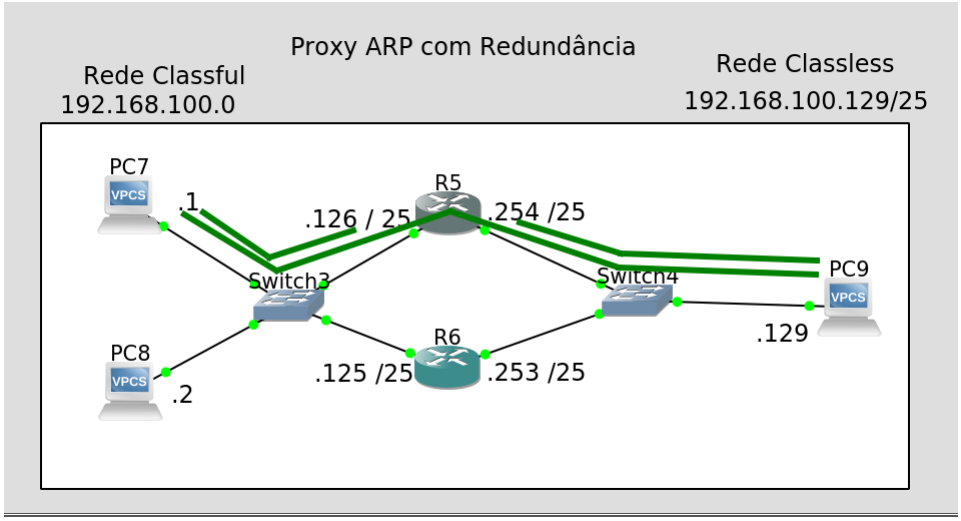
- Neste caso a rede A é uma rede classful (não tem máscara) e a rede B é uma rede classless (tem máscara). Caso o PC2 queira comunicar com o PC3 o R3 tem de alguma forma ajudar nesse processo porque o PC2 vai pensar que está na mesma rede que o PC3 e vai tentar fazer um **ARP Request** para o PC3 diretamente.
- O PC2 envia um **ARP Request** em broadcast mas como o PC3 está noutro dominio de difusão o mesmo nunca vai responder pois neste caso o R3 está com o **proxy arp** desligado.
- Então é aqui que entra o **proxy arp**, que faz com que o R3 responda ao **ARP Request**,como se fosse o PC3, com um **ARP Response**.
- Depois disto o PC2 vai mapear uma tabela de arp que diz que o IP do PC3 corresponde ao MAC do R3, pois o R3 é o proxy.
- O **proxy arp** é ativado na interface que está virada para a rede classful



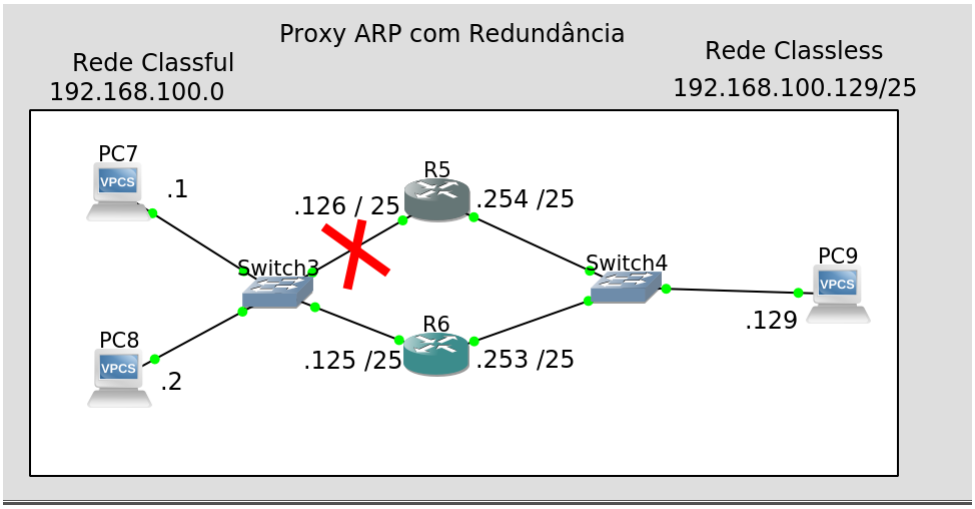
- A cache ARP não é actualizada no momento em que ocorre um problema com o default gateway de serviço
- Quando a entrada expira o mecanismo de Proxy ARP de outro router pode substituir o router avariado
- O tempo por omissão da tabela arp nos routers da cisco é cerca de 4 horas, podendo ser alterado usando o comando `arp timeout [numero]`

Utilizando redundância com o Proxy ARP

- Para utilizar a redundancia foi colocado um segundo router no entanto a topologia está configurada para utilizar o R5 tanto para **Echo Requests** como para **Echo Replys** , sendo que o R5 tem o **proxy arp** ativo, logo o PC7 consegue comunicar com o PC9.



- Para testar a redundância, foi desligado a *e0/0* do R5 como mostra a figura



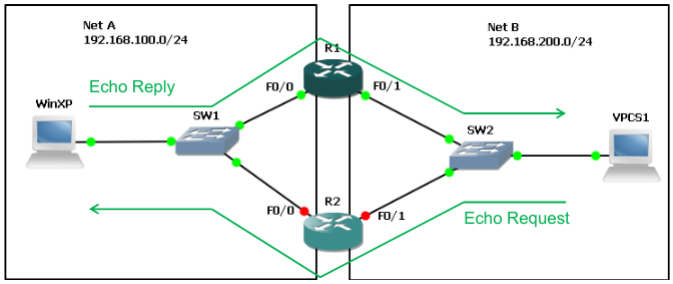
- Depois de desligada a interface consegue-se reparar que o *ping* do PC7 para o PC9 deixa de funcionar

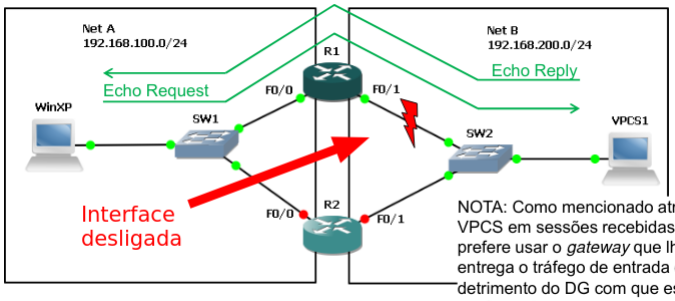
- Uma maneira para resolver este problema seria colocar no PC9 como *default gateway* o R6, sendo que este teria o **proxy arp** ativo.

Usando RIP Listeners

- Uma maneira de tolerar falhas no *default gateway* é por exemplo utilizar o **RIP** como protocolo de encaminhamento e os PCS conterem um **Agente RIP** que faz com que caso exista uma falha no *default gateway* o mesmo tenta verificar se existe mais algum

router a enviar trafego RIP e faz desse o seu *default gateway*.





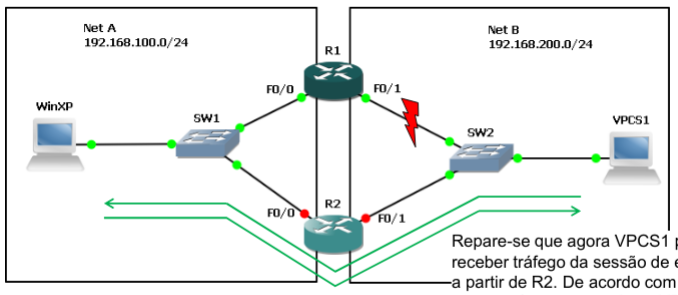
NOTA: Como mencionado atrás, o VPCS em sessões recebidas prefere usar o *gateway* que lhe entrega o tráfego de entrada em detrimento do DG com que está configurado.

```
C:\Documents and Settings\Cisco>ping -t 192.168.200.1

Pinging 192.168.200.1 with 32 bytes of data:

Reply from 192.168.200.1: bytes=32 time=37ms TTL=63
Reply from 192.168.200.1: bytes=32 time=25ms TTL=63
Reply from 192.168.200.1: bytes=32 time=25ms TTL=63
Reply from 192.168.200.1: bytes=32 time=50ms TTL=63
Reply from 192.168.200.1: bytes=32 time=34ms TTL=63
Reply from 192.168.200.1: bytes=32 time=38ms TTL=63
Reply from 192.168.200.1: bytes=32 time=22ms TTL=63
=> Desligado
Reply from 192.168.100.254: Destination host unreachable.
Reply from 192.168.100.254: Destination host unreachable.
Reply from 192.168.100.254: Destination host unreachable.
Reply from 192.168.100.254: Destination host unreachable.
Reply from 192.168.100.254: Destination host unreachable.
Reply from 192.168.100.254: Destination host unreachable.
Reply from 192.168.100.254: Destination host unreachable.
Reply from 192.168.100.254: Destination host unreachable.
Reply from 192.168.100.254: Destination host unreachable.
Reply from 192.168.100.254: Destination host unreachable.
Reply from 192.168.100.254: Destination host unreachable.
Reply from 192.168.200.1: bytes=32 time=101ms TTL=63
Reply from 192.168.200.1: bytes=32 time=21ms TTL=63
```

15 s



Repare-se que agora VPCS1 passa a receber tráfego da sessão de entrada a partir de R2. De acordo com as notas atrás apresentadas o VPCS passará agora a usar R2 como *gateway* para o tráfego de resposta.