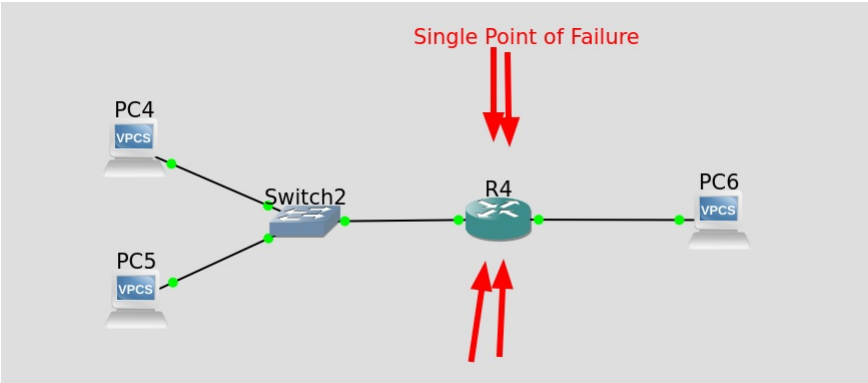


# Single Point of Failure



- 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 disponível
- 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

### 2 Routers - 2 DHCP Servers

192.168.1.0/24

Wireshark capture of DHCP traffic:

No.	Time	Source	Destination	Protocol	Length	Info
5	57.925455	0.0.0.0	255.255.255.255	DHCP	406	DHCP
8	58.925858	0.0.0.0	255.255.255.255	DHCP	406	DHCP
11	59.946954	192.168.1.253	192.168.1.1	DHCP	342	DHCP
12	59.948929	192.168.1.254	192.168.1.1	DHCP	342	DHCP
13	61.926222	0.0.0.0	255.255.255.255	DHCP	406	DHCP
14	61.927266	192.168.1.253	192.168.1.1	DHCP	342	DHCP

Frame 14: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface  
 Ethernet II, Src: aa:bb:cc:00:01:00 (aa:bb:cc:00:01:00), Dst: Private\_66:68:00  
 Internet Protocol Version 4, Src: 192.168.1.253, Dst: 192.168.1.1  
 User Datagram Protocol, Src Port: 67, Dst Port: 68  
 Dynamic Host Configuration Protocol (ACK)

PC1 terminal output:

```

Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.

Welcome to Virtual PC Simulator, version 0.8.2
Dedicated to Daling.
Build time: Aug 23 2021 11:15:00
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

PC1> ip dhcp
DDORA IP 192.168.1.1/24 GW 192.168.1.253

```

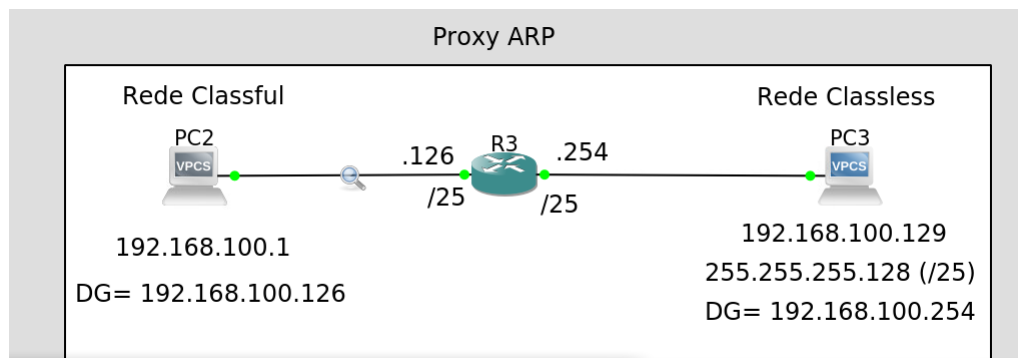
## Proxy ARP

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 domínio 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

~ [PC2 Ethernet0 to R3 Ethernet0/0]

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp

No.	Time	Source	Destination	Protocol	Length	Info
3	14.716466	Private 66:68:01	Broadcast	ARP	64	Who has 192.168.100.129? Tell 192.168.100.1
4	14.717634	aa:bb:cc:00:03:00	Private 66:68:01	ARP	60	192.168.100.129 is at aa:bb:cc:00:03:00

Frame 3: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface -, id 0  
 Ethernet II, Src: Private\_66:68:01 (00:50:79:66:68:01), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
 Address Resolution Protocol (request)

```

0000  ff ff ff ff ff 00 50 79 66 68 01 00 06 00 01 ..... P yfh....
0010  00 00 06 04 00 01 00 50 79 66 68 01 c0 a8 64 01 ..... P yfh....d
0020  ff ff ff ff ff c0 a8 64 81 00 00 00 00 00 00 ..... d.....
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
  
```

PC2

/bin/bas

Copyright (c) 2007-2015, Paul Meng (mirnsh)

All rights reserved.

VPCS is free software, distributed under t

Source code and license can be found at vp

For more information, please visit wiki.fr

Press '?' to get help.

Executing the startup file

Checking for duplicate address...

PC2 : 192.168.100.1 255.255.255.0 gateway

PC2> ping 192.168.100.129

84 bytes from 192.168.100.129 icmp\_seq=1 t

84 bytes from 192.168.100.129 icmp\_seq=2 t

84 bytes from 192.168.100.129 icmp\_seq=3 t

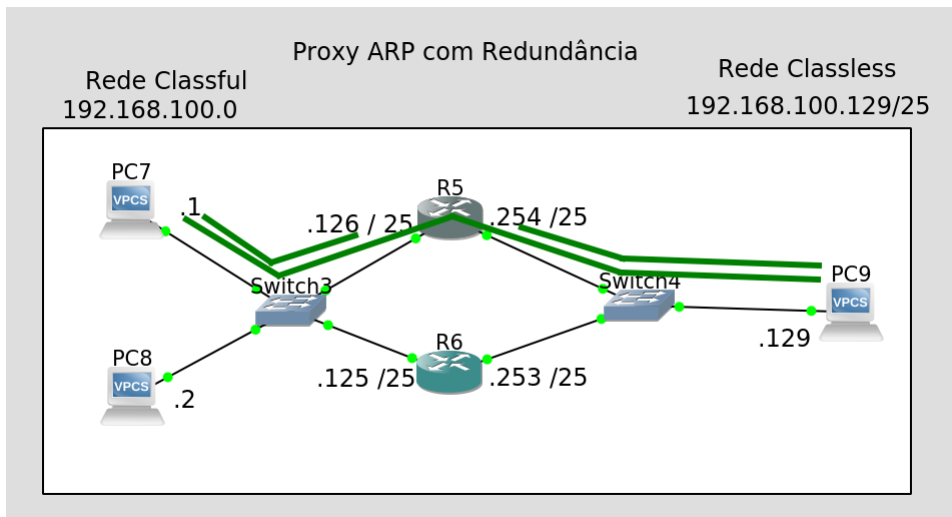
84 bytes from 192.168.100.129 icmp\_seq=4 t

84 bytes from 192.168.100.129 icmp\_seq=5 t

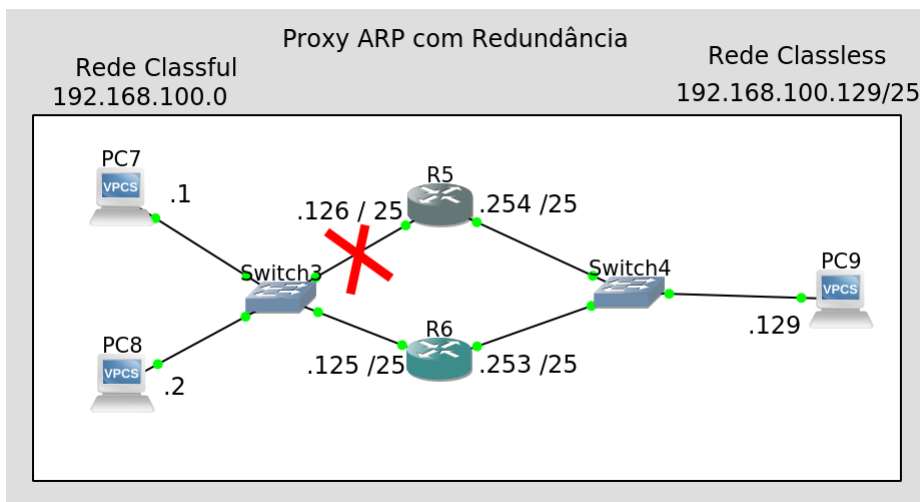
- A cache ARP não é atualizada no momento em que ocorre um problema com o default gateway de serviço
- Quando a entrada expira o mecanismo de Proxy ARP de outro router pode substituir o router avariado
- O tempo por omissão da tabela arp nos routers da cisco é cerca de 4 horas, podendo ser alterado usando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

## Utilizando redundância com o Proxy ARP

- Para utilizar a redundância foi colocado um segundo router no entanto a topologia está configurada para utilizar o R5 tanto para **Echo Requests** como para **Echo Replies**, 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

```

PC7> ping 192.168.100.129
192.168.100.129 icmp_seq=1 timeout
192.168.100.129 icmp_seq=2 timeout
192.168.100.129 icmp_seq=3 timeout
192.168.100.129 icmp_seq=4 timeout
192.168.100.129 icmp_seq=5 timeout
  
```

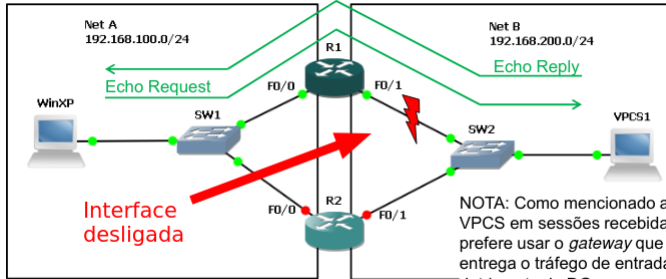
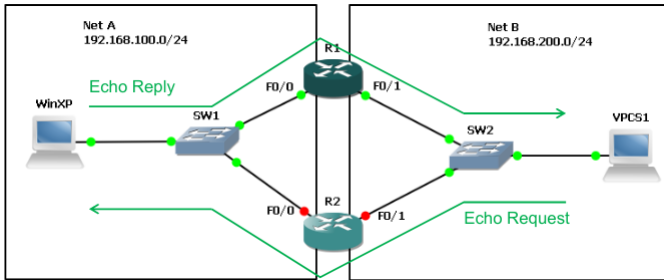
Interface	IP-Address	OK?	Method	Status
Ethernet0/0	192.168.100.126	YES	manual	adminis
Ethernet0/1	192.168.100.254	YES	manual	up
Ethernet0/2	unassigned	YES	NVRAM	adminis
Ethernet0/3	unassigned	YES	NVRAM	adminis
Ethernet1/0	unassigned	YES	NVRAM	adminis
Ethernet1/1	unassigned	YES	NVRAM	adminis
Ethernet1/2	unassigned	YES	NVRAM	adminis

- 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 na **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 na **default gateway** o mesmo tenta verificar se existe mais algum

router a enviar tráfego 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

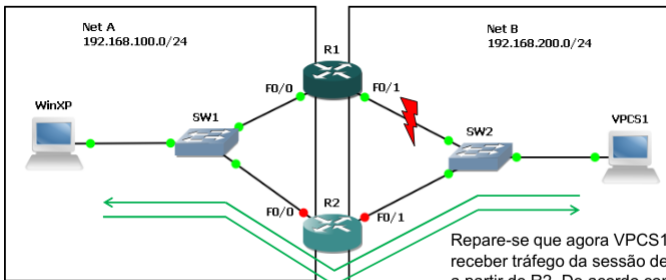
Pinging 192.168.200.1 with 32 bytes of data:

```
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 192.168.100.254: 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.