

# REDES E SERVIÇOS

---

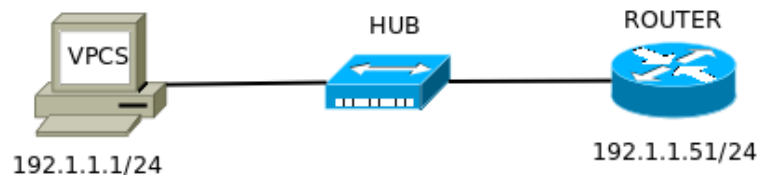
## Objetivos

- Familiarização com a configuração de switches Ethernet e com routers IP.
- Estudo dos processos de expedição de pacotes em switches Ethernet e routers IP.

## Experiências com *hubs* e *switches*

1. Monte a rede Ethernet baseada num *hub* que está ilustrada na figura seguinte e configure os endereços IP nos equipamentos. Teste a conectividade entre o PC e Router através do comando *ping* (executado no PC e no Router).

Nas experiências da secção 2 deste guia, o *router* é usado apenas como equipamento terminal. Considere os endereços IP de classe C (máscara 255.255.255.0 ou /24) em que a parte de *host* depende do número atribuído a cada grupo da seguinte forma:



### Configuração do *router*

Os routers têm múltiplos interfaces cada um com um nome atribuído. De modo a saber o nome dos interfaces do seu *router* execute o comando `show interfaces`. Para configurar o endereço IP num interface do *router* introduza os seguintes comandos:

```
router>enable
router#
router#configure terminal
router(config)#
router(config)#interface fastethernet0/0          !O nome do interface que está em uso
router(config-if)#ip address 192.1.1.51 255.255.255.0
router(config-if)#no shutdown
router(config-if)#end
router#write
Building configuration...
[OK]
router#
```

2. Inicie uma captura com o filtro de visualização “*icmp*” e execute o comando *ping* para o endereço do *router*. Observe os dois níveis de encapsulamento: a mensagem ICMP é encapsulada num datagrama IP que é por sua vez encapsulado numa trama Ethernet. Registe a seguinte informação:

- Endereço MAC da placa de rede do PC:
- Endereço MAC do interface do *Router* em utilização:
- Código hexadecimal (campo *Type* do cabeçalho Ethernet) que identifica os dados como sendo um pacote IP:
- Código hexadecimal (campo *Protocol* do cabeçalho IP) que identifica os dados como sendo um pacote ICMP:
- Código hexadecimal (campo *Type* do cabeçalho ICMP) que identifica os dois tipos de pacotes ICMP capturados (*Echo Request* e *Echo Reply*):

3. Inicie uma nova captura com o filtro de visualização “icmp or arp”. Execute o comando

```
arp
```

para consultar a tabela ARP do seu VPCS. Espere cerca de 2 minutos para que a entrada do endereço IP do *router* na tabela ARP do VPCs seja apagada). Consulte novamente a tabela ARP do seu PC. Execute o comando

```
ping 192.1.1.51
```

e torne a verificar a tabela ARP. Analise os campos seguintes dos pacotes ARP capturados e, com base nos seus valores, explique o protocolo ARP:

<b>ARP Request</b>	Cabeçalho do pacote Ethernet	Endereço Origem: Endereço Destino:
	Conteúdo do pacote ARP	Endereço MAC Origem: Endereço IP Origem: Endereço MAC Destino: Endereço IP Destino:
<b>ARP Response</b>	Cabeçalho do pacote Ethernet	Endereço Origem: Endereço Destino:
	Conteúdo do pacote ARP	Endereço MAC Origem: Endereço IP Origem: Endereço MAC Destino: Endereço IP Destino:

4. Certifique-se que a entrada do endereço IP do *router* na tabela ARP do VPCS está apagada. Execute agora o comando

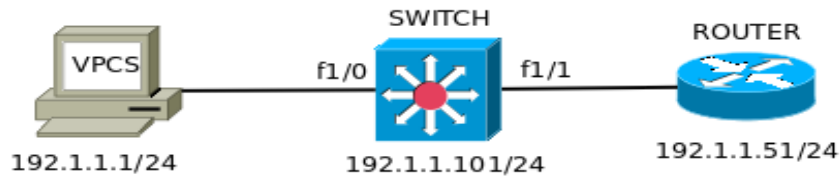
```
ping 192.1.1.51 -l 5
```

Verifique e explique o processo de *padding* em ambos os pacotes ARP e ICMP capturados.

**Nota 1:** O processo de *padding* consiste na introdução de zeros no final da conteúdo da trama Ethernet de modo a esta ter o tamanho mínimo imposto pela norma (64 bytes, including 4 bytes for CRC). O *padding* dos pacotes com origem no PC não será visível devido ao ponto onde o Wireshark captura os pacotes (antes da introdução do *padding*).

## Experiências de *switching*

5. Monte uma rede Ethernet que interligue um PC e um *router* através de um *switch* Ethernet. Configure todos os equipamentos com os endereços IP especificados na figura. Teste a conectividade de cada um dos equipamentos para os restantes dois através do comando *ping*.



### Configuração do Endereço IP do *switch*

O endereço IP do *switch* será configurado na VLAN 1, a VLAN por omissão.

```
R2-SW#configure terminal
R2-SW#(config)#interface vlan 1
R2-SW#(config-if)#ip address 192.1.1.101 255.255.255.0
R2-SW(config-if)#no shutdown
R2-SW(config-if)#end
R2-SW#write
Building configuration...
[OK]
R2-SW#
```

6. Execute novamente o comando *ping* entre o PC e o *router*. Consulte a tabela de encaminhamento do *switch* utilizando o comando: *show mac-address-table*

Registre o seu conteúdo e justifique. Com base no conteúdo da tabela de encaminhamento, registre quais os endereços MAC do PC e da interface do *router* ligada.

7. O tempo de vida das entradas da tabela de encaminhamento (*MAC Aging Time*) do *switch* pode ser configurado. Usando o comando

```
show mac-address-table aging-time
```

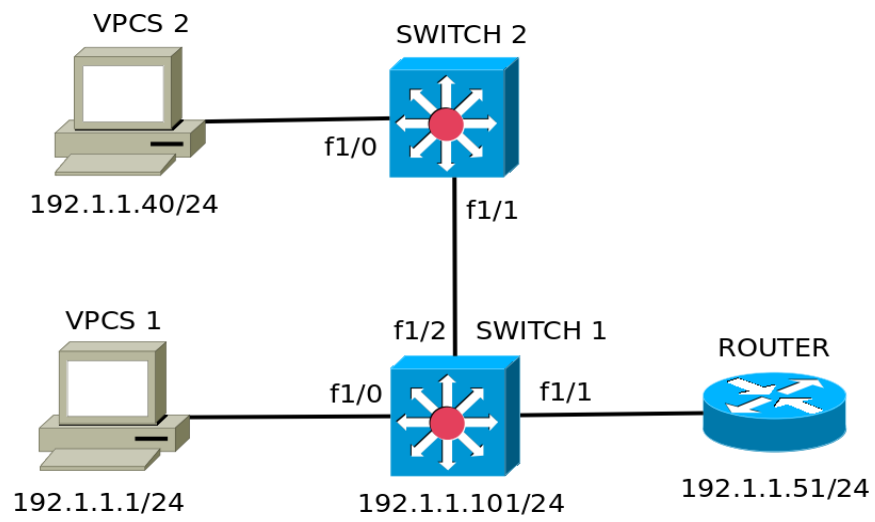
registre o valor de *Aging Time* que está configurado por omissão. Configure um *Aging Time* de 10 segundos:

```
mac-address-table aging-time 10
```

Espere cerca de 15 segundos e verifique se o endereço do PC desaparece da tabela de encaminhamento.<sup>1</sup>

8. Acrescente à sua rede uma ligação a um novo *switch* que por sua vez está ligado a um segundo VPCS. Na ligação ao VPCS 1, inicie uma captura com o filtro de visualização “icmp” e faça um *ping* do *router* para o VPCS 2. Registre que pacotes capturou e explique o sucedido com base nos processos de *flooding* e *forwarding* do *switch*.

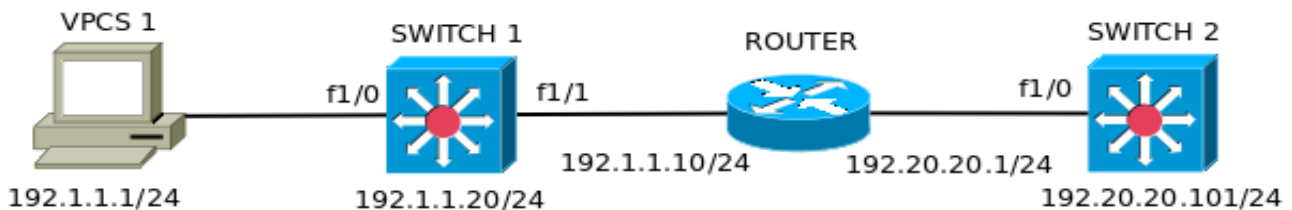
<sup>1</sup> O endereço MAC do *router* não desaparece da tabela de encaminhamento pela seguinte razão: os *routers* enviam periodicamente (de 10 seg. em 10 seg.) um pacote de LOOPBACK para verificarem se têm conectividade física; estes pacotes validam continuamente o endereço MAC do *router* no *switch*.



## Experiências de *routing*

9. Monte a rede da figura seguinte, constituída por duas redes IP interligadas através de um *router*. Não configure nenhum *Default Gateway* nos equipamentos terminais. Consulte e registre a tabela de encaminhamento do *router*.

Note que o *switch* é usado apenas como estação terminal.



### Leitura de tabelas de encaminhamento em routers Cisco

As tabelas de encaminhamento dos *routers* podem ser consultadas através do comando *show ip route*. As entradas da tabela de encaminhamento têm o seguinte significado:

C	2.0.0.0/8 is directly connected, Ethernet0	
		Indica como foi obtida a entrada, C para ligações directas do <i>router</i>
		Endereço da rede destino e o nº de bits mais significativos da máscara a '1' (ex.: 2.0.0.0/8, para uma máscara de 255.0.0.0).
		Interface por onde deve ser enviado um pacote para aquela rede de destino.

10. Inicie uma captura com o filtro de visualização “icmp” na ligação entre o *switch* 1 e o VPCS. Execute o comando *ping* do VPCS para o *switch* 2. Justifique o resultado da captura efectuada. Repita a experiência com o comando *ping* a ser gerado do *switch* 2 (via consola) para o VPCS.

11. Configure o *Default Gateway* no *switch* com o endereço IP da porta do *router* a que está ligado. Não configure o *Default Gateway* do VPCS. Inicie nova captura com o filtro “icmp” e execute um comando *ping* do *switch* 2 para o VPCS. Registe e justifique a resposta do comando *ping* e os pacotes que foram capturados.

### Configuração do Default Gateway do switch:

```
SW# ip default-gateway 192.20.20.1
```

12. Configure agora o *Default Gateway* no VPCS com o endereço IP da porta do *router* a que está ligado. Inicie nova captura com o filtro de visualização “icmp” e execute um comando *ping* do VPCS para o *switch* 2. Verifique se existe conectividade entre o *switch* e o VPCS. Justifique o que observou nas experiências 10, 11 e 12.

## Configuração do Default Gateway no VPCS:

```
ip 192.1.1.1/24 192.1.1.10
```

13. Inicie uma captura com o filtro de visualização “icmp or arp” e execute um comando *ping do switch 2* para uma rede IP inexistente. Registre que pacotes foram capturados. O que pode concluir relativamente à diferença entre os processos de expedição de pacotes em *switches* e em *routers*?

14. Reinicie uma captura com o filtro de visualização “icmp or arp” e execute o comando *ping do switch 2* para um endereço inexistente da rede IP do VPCS. Registre que pacotes que foram capturados e explique o sucedido.

15. Inicie uma captura com o filtro de visualização “icmp or arp” e execute um comando *ping do VPCS* para uma rede IP inexistente. Registre que pacotes foram capturados. O que pode concluir relativamente à diferença entre os processos de expedição de pacotes em *switches* e em *routers*?