



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.

Duração

2 aulas

Documentos adicionais necessários para a execução do guia

- Comandos de Configuração do *Router* Cisco
- Comandos de Configuração do *Switch* D-Link

Os protocolos ARP e ICMP

1. Com os equipamentos desligados, monte a rede Ethernet da figura seguinte. Seguidamente, ligue os equipamentos (o PC deverá ser arrancado com o SO Linux) e configure-os como especificado.

Para configurar o endereço IP no PC use numa janela terminal os comandos:

```
PC:~$ sudo service network-manager stop
PC:~$ sudo ifconfig eth0 up
PC:~$ sudo ifconfig eth0 192.1.1.x/24
```

Nota1: Estes comandos desligam o gestor de interfaces de redes do Linux, ligam o interface eth0 e definem o endereço IPv4 do mesmo.

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*

Para configurar o *router* é necessário ligar a porta da consola do *router* à porta série/USB do PC (utilizando o cabo e adaptador apropriado) e utilizar o programa *minicom*. Utilizando (numa janela terminal do PC) o comando:

```
PC:~$ sudo minicom
```

Ligue o *router* e pressione a tecla *Enter* algumas vezes até aparecer:

```
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 -n
```

para consultar a tabela ARP do seu PC. Execute o comando

```
sudo arp -d 192.1.1.51
```

para apagar a entrada do endereço IP do *router* na tabela ARP do PC, se esta existir). 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:

ARP Request	Cabeçalho do pacote Ethernet	Endereço Origem:
		Endereço Destino:
	Conteúdo do pacote ARP	Endereço MAC Origem:
		Endereço IP Origem:
		Endereço MAC Destino:
		Endereço IP Destino:
ARP Response	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. Inicie uma captura com o filtro de visualização “icmp or arp”. Execute novamente o comando

```
arp -d 192.1.1.51
```

para apagar a entrada do endereço IP do *router* na tabela ARP do PC, se esta existir. Execute agora o comando

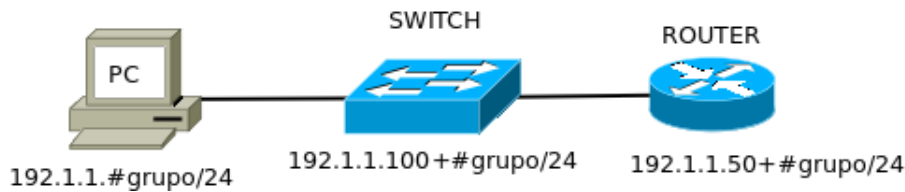
```
ping -s 5 192.1.1.51
```

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*.



Nota: x deverá ser substituído pelo seu número de grupo (#grupo).

Configuração do Endereço IP do switch

Para configurar o *switch* é necessário ligar a porta da consola (RS-232) do *switch* à porta série/USB do PC (utilizando o cabo de consola do *switch*). Utilizando o terminal *minicom* (pode continuar a usar o mesmo terminal usado na configuração do *router*), pressione a tecla *Enter* algumas vezes até aparecer:

```
Switch#
```

Utiliza o seguinte comando para definir o endereço IPv4 do *switch*:

```
Switch# config ipif System ipaddress 192.1.1.x/24
```

6. Execute novamente o comando *ping* entre o PC e o *router*. Consulte a tabela de encaminhamento do *switch*:

- via *web browser* acedendo ao interface web do *switch*: endereço `http://192.1.1.#grupo+100`, clicando em *Login* (sem *password*) e acedendo ao menu *Monitoring* → *MAC addresses*.

- via consola: utilizando o comando: `show fdb`

Registe o seu conteúdo e justifique. Com base no conteúdo da tabela de encaminhamento, registe 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 fdb aging_time
```

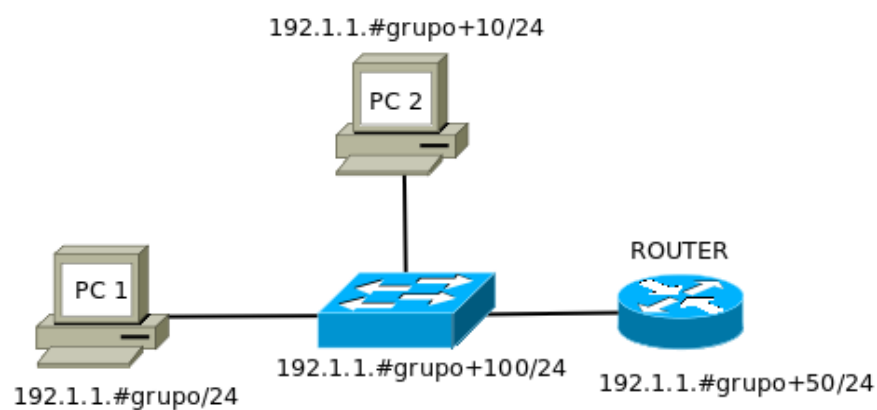
registe o valor de *Aging Time* que está configurado por omissão. Configure um *Aging Time* de 10 segundos:

```
config fdb aging_time 10
```

Espere cerca de 20 segundos e verifique se o endereço do PC desaparece da tabela de encaminhamento (via *web browser* e via consola).¹

¹ 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*.

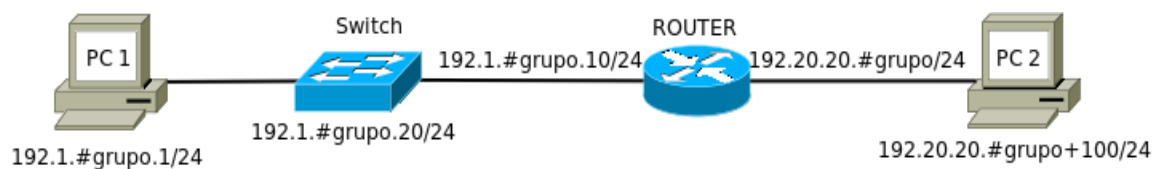
8. Acrescente à sua rede uma ligação entre o seu *switch* e um segundo PC. No PC1, inicie uma captura com o filtro de visualização “icmp” e faça um *ping* do *router* para o PC2. Registe que pacotes capturou e explique o sucedido com base nos processos de *flooding* e *forwarding* do *switch*.



Experiências de *routing*

9. Monte duas redes IP interligadas através de um *router* e configure os equipamentos com os endereços especificados na figura (sem configurar nenhum *Default Gateway*). Consulte e registre a tabela de encaminhamento do *router*.

Nesta experiência, os endereços IP a usar devem ser de classe C (máscara 255.255.255.0) e dependem do número atribuído a cada Grupo de trabalho da seguinte forma:



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”. Execute o comando *ping* do PC1 para o PC2. Justifique o resultado da captura efectuada. Repita a experiência com o comando *ping* a ser gerado do PC2 (via consola) para o PC1.

11. Configure o *Default Gateway* no PC2 com o endereço IP da porta do *router* a que está ligado. Não configure o *Default Gateway* do PC1. Inicie nova captura com o filtro “icmp” e execute um comando *ping* do PC2 para o PC. Registre e justifique a resposta do comando *ping* e os pacotes que foram capturados.

Configuração do Default Gateway do switch:

```
Switch# create iproute default 192.20.20.#grupo
```

12. Configure agora o *Default Gateway* no PC1 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 PC1 para o PC2. Verifique se existe conectividade. Justifique o que observou nas experiências 10, 11 e 12.

Configuração do Default Gateway no PC Linux:

```
PC:~$ sudo route add default gw 192.1.#grupo.10
```

13. Inicie uma captura com o filtro de visualização “icmp or arp” e execute um comando *ping* do PC2 para uma rede IP inexistente. Registe 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 PC2 para um endereço inexistente da rede IP do PC. Registe 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 PC1 para uma rede IP inexistente. Registe que pacotes foram capturados. O que pode concluir relativamente à diferença entre os processos de expedição de pacotes em *switches* e em *routers*?