

# RS - RESUMOS PRÁTICAS 2

## AULA 06

Organizando os dispositivos conforme a figura do guião, configuramos o router para ter o endereço ipv6 2001:A:1:1::100/64. Inicialmente, o PC1 possui apenas o link-local scope mas, após introduzir endereço anterior no router, o PC1 obtém um global scope com o prefixo do endereço do router anunciado (2001:A:1:1:) sendo que os restantes valores (sufixo) são originados automaticamente através do padrão eui-64.

De seguida adicionamos um novo endereço ipv6 ao router: 2001:A:1:2::/64 eui-64. Verifica-se através do Wireshark que o router passa a anunciar dois prefixos – 2001:A:1:1 e 2001:A:1:2 – ambos endereços globais. Assim, espera-se que o PC1 configure novamente um novo endereço global. Contudo, o PC1 é um terminal básico que não suporta mais do que um endereço global e, por isso, este segundo endereço não vai aparecer (num pc normal isto podia acontecer).

```
PC1> ping FE80::C801:FFF:FEB5:0
FE80::C801:FFF:FEB5:0 icmp6_seq=1 ttl=64 time=19.042 ms
FE80::C801:FFF:FEB5:0 icmp6_seq=2 ttl=64 time=4.399 ms
FE80::C801:FFF:FEB5:0 icmp6_seq=3 ttl=64 time=16.695 ms
FE80::C801:FFF:FEB5:0 icmp6_seq=4 ttl=64 time=10.312 ms
FE80::C801:FFF:FEB5:0 icmp6_seq=5 ttl=64 time=5.243 ms

PC1> ping 2001:A:1:1::100
2001:A:1:1::100 icmp6_seq=1 ttl=64 time=10.148 ms
2001:A:1:1::100 icmp6_seq=2 ttl=64 time=7.714 ms
2001:A:1:1::100 icmp6_seq=3 ttl=64 time=10.232 ms
2001:A:1:1::100 icmp6_seq=4 ttl=64 time=8.104 ms
2001:A:1:1::100 icmp6_seq=5 ttl=64 time=5.276 ms

PC1> ping 2001:A:1:2:C801:FFF:FEB5:0
host (2001:A:1:2:C801:FFF:FEB5:0) not reachable
```

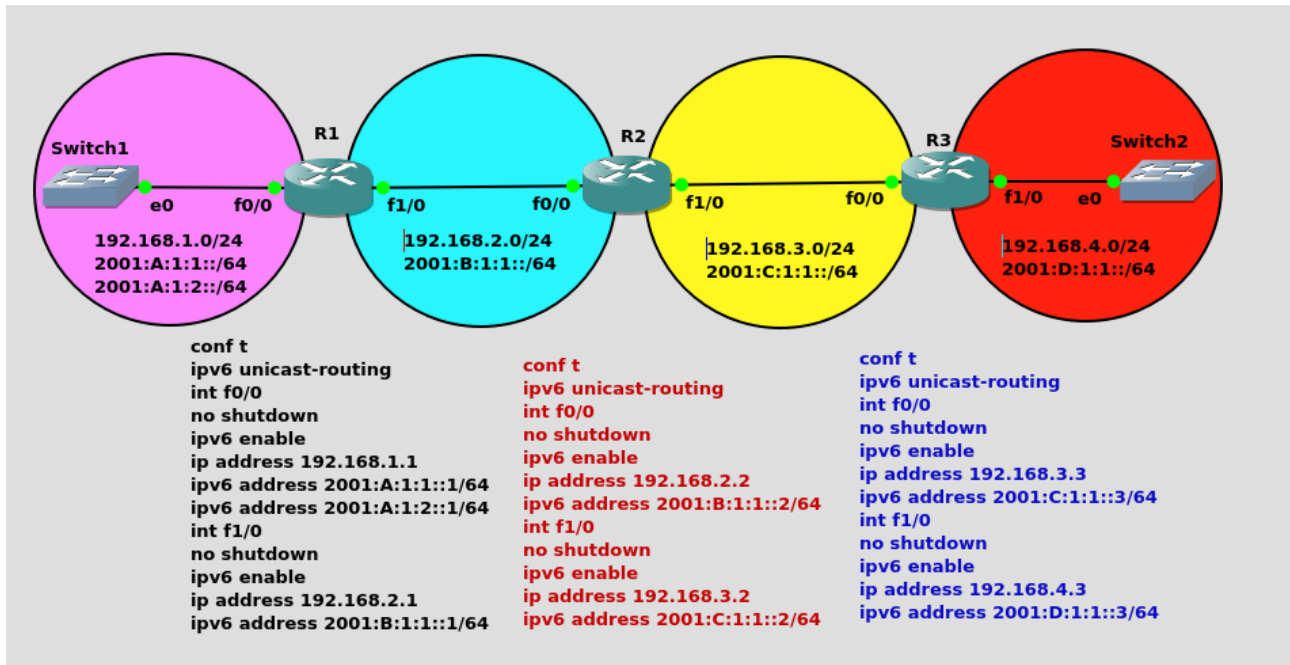
Tal como era esperado, ao fazer ping do PC1 para um endereço 2001:1:2:(sufixo), não vai haver conexão entre ambos os terminais, uma vez que o PC1 tem apenas o endereço 2001:1:1... como endereço global e não 2001:1:2...

Fazendo ping ao link local address do router, vai haver ICMPv6 Request e ICMPv6 Reply. No entanto, quando fazemos ping ao global address do router, verifica-se através do Wireshark um Neighbour Solicitation do PC para o Router (uma vez que não conhece o MAC address do router) e um Neighbour Advertisement do Router para o PC (envia o endereço MAC de volta para o computador). Este processo é semelhante ao ARP Request/Reply do ipv4. Possuindo agora o endereço MAC do router, já se verifica os pacotes ICMPv6 Request e Reply.

Introduzindo “show ipv6 interface brief” aparece a lista de endereços ipv6 do router da respetiva interface (f0/0). Outros comandos: “show ipv6 route” (mostra uma tabela com as rotas) e “show ipv6 interface” (informação sobre a interface).

Conclui-se assim a primeira parte da aula 06 destinada a perceber os mecanismos básicos do IPv6.

Na figura seguinte temos um conjunto de redes configuradas com endereços IPv4 e IPv6.



Realizando os comandos “show ip arp/route/int brief”, verifica-se tal como era esperado que o R1 só conhece as redes que lhe são adjacentes (primeira e segunda).

```
R1#show ip int brief
Interface                IP-Address      OK? Method Status  Protocol
FastEthernet0/0          192.168.1.1     YES NVRAM  up      up
FastEthernet1/0          192.168.2.1     YES manual  up      up
FastEthernet2/0          unassigned      YES NVRAM  administratively down down
FastEthernet2/1          unassigned      YES NVRAM  administratively down down
```

Realizando os mesmos comandos para ipv6 verifica-se o mesmo, sendo que ao introduzir o comando “show ipv6 int brief aparecem as interfaces ativas bem como os respetivos link-local scope e global-scopes.

```
R1#show ipv6 int brief
FastEthernet0/0          [up/up]
FE80::C801:12FF:FE1B:0
2001:A:1:1::1
2001:A:1:2::1
FastEthernet1/0          [up/up]
FE80::C801:12FF:FE1B:1C
2001:B:1:1::1
FastEthernet2/0          [administratively down/down]
unassigned
FastEthernet2/1          [administratively down/down]
unassigned
```

Assim, cada router representado no esquema conhece apenas as redes que lhe são adjacentes. Adiciona-se agora as seguintes configurações para cada um dos routers:

*ip route <nome da rede ipv4 que queremos conetar> <máscara de rede ipv4> <default-gateway da rede atual>*  
*ipv6 route <rede ipv6 que queremos conetar> <"default-gateway" da rede atual ipv6>*

**R1:**

```
conf t
ip route 192.168.3.0 255.255.255.0 192.168.2.2
ip route 192.168.4.0 255.255.255.0 192.168.2.2
ipv6 route 2001:C:1:1::/64 2001:B:1:1::2
ipv6 route 2001:D:1:1::/64 2001:B:1:1::2
```

**R2:**

```
conf t
ip route 192.168.1.0 255.255.255.0 192.168.2.1
ip route 192.168.4.0 255.255.255.0 192.168.3.2
ipv6 route 2001:A:1:1::/64 2001:B:1:1::1
ipv6 route 2001:A:1:2::/64 2001:B:1:1::1
ipv6 route 2001:D:1:1::/64 2001:C:1:1::3
```

**R3:**

```
conf t
ip route 192.168.1.0 255.255.255.0 192.168.3.2
ip route 192.168.2.0 255.255.255.0 192.168.3.2
ipv6 route 2001:A:1:1::/64 2001:C:1:1::2
ipv6 route 2001:A:1:2::/64 2001:C:1:1::2
ipv6 route 2001:B:1:1::/64 2001:C:1:1::2
```

Terminando de configurar as rotas estáticas para atingir conectividade total ipv4 e ipv6 entre todos os aparelhos (agora os routers já “conhecem” as restantes redes), podemos prosseguir à captura de dados no Wireshark.

Analisando o fluxo de dados entre R2 e R3 e introduzindo a partir do R1 o endereço ipv4 de R3, verifica-se que circulam dois tipos de pacotes: ICMP Request (R1→R3) e ICMP Reply (R3→R1), sendo que antes disto há uma troca de pacotes ARP Request/Reply. O pacote ICMP Request tem como endereço ipv4 de origem 192.168.2.1 e de destino 192.168.4.0 (como era esperado).

O mesmo processo ocorre para quando fazemos ping com endereços ipv6. Existe circulação de pacotes Neighbor Solicitation / Neighbor Advertisement e ICMPv6 Request/Reply.

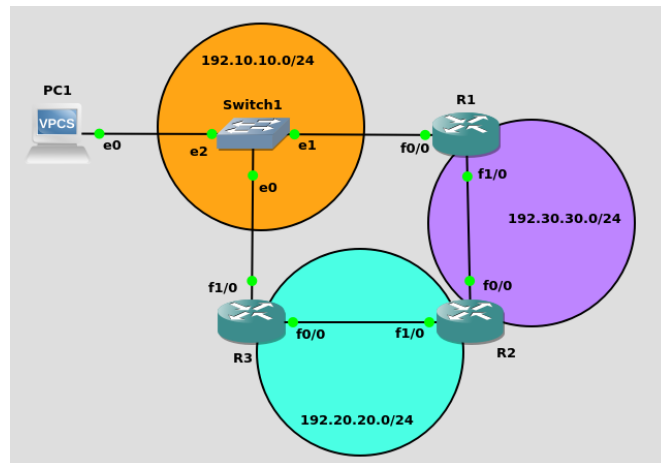
O que é proposto no exercício 8 é apenas uma forma de fazer os exercícios 6 e 7 de uma forma mais simplificada.

Desta forma, verifica-se que há conectividade entre todas as redes, inserindo tanto endereços ipv4 como ipv6, uma vez que definimos rotas estáticas (static routing). Assim, para estabelecer conexão entre todas as redes, o administrador da rede tem de inserir manualmente estas rotas estáticas.

## AULA 07

### Protocolo RIP

Montando a rede e configurando cada um dos routers para suportar o Routing Information Protocol (adicionando as redes diretamente ligadas ao respectivo router e configurando um IP para cada uma das interfaces do router), obtemos o esquema seguinte:



Usando o comando “show ip route” para cada router (R1 / R2 / R3):

```
C 192.30.30.0/24 is directly connected, FastEthernet1/0
C 192.10.10.0/24 is directly connected, FastEthernet0/0
R 192.20.20.0/24 [120/1] via 192.30.30.2, 00:00:11, FastEthernet1/0
[120/1] via 192.10.10.2, 00:00:16, FastEthernet0/0
```

```
C 192.30.30.0/24 is directly connected, FastEthernet0/0
R 192.10.10.0/24 [120/1] via 192.30.30.1, 00:00:17, FastEthernet0/0
[120/1] via 192.20.20.1, 00:00:27, FastEthernet1/0
C 192.20.20.0/24 is directly connected, FastEthernet1/0
```

```
R 192.30.30.0/24 [120/1] via 192.20.20.2, 00:00:16, FastEthernet0/0
[120/1] via 192.10.10.1, 00:00:11, FastEthernet1/0
C 192.10.10.0/24 is directly connected, FastEthernet1/0
C 192.20.20.0/24 is directly connected, FastEthernet0/0
```

Cada um dos routers mostra a rede a que está diretamente conetado (C), bem como as respetivas redes conhecidas através do protocolo RIP (R), uma vez que as redes diretamente conetadas vão enviar informação sobre as redes vizinhas que o router “original” não conhece (ip da rede + vetor distância + ip da interface do router através da qual se chega a essa rede, etc...).

Iniciando captura na rede 192.10.10.0, captura-se periodicamente (30s) pacotes do tipo Response com as respetivas informações sobre a rede, o vetor distância, etc...

4	22.579653	192.10.10.2	255.255.255.255	RIPv1	66	Response
5	22.841574	192.10.10.1	255.255.255.255	RIPv1	66	Response
10	48.572576	192.10.10.2	255.255.255.255	RIPv1	66	Response
12	52.051031	192.10.10.1	255.255.255.255	RIPv1	66	Response
15	77.600609	192.10.10.1	255.255.255.255	RIPv1	66	Response
16	77.680032	192.10.10.2	255.255.255.255	RIPv1	66	Response
22	104.362946	192.10.10.2	255.255.255.255	RIPv1	66	Response
23	104.925376	192.10.10.1	255.255.255.255	RIPv1	66	Response

Nas figuras seguintes temos a informação relativa ao RIP da interface da rede 192.10.10.0 correspondente a R1 com split-horizon (figura da esquerda) e sem split-horizon (figura da direita):

<pre> ▼ Routing Information Protocol   Command: Response (2)   Version: RIPv1 (1)   ▼ IP Address: 192.30.30.0, Metric: 1     Address Family: IP (2)     IP Address: 192.30.30.0     Metric: 1         </pre>	<pre> ▼ Routing Information Protocol   Command: Response (2)   Version: RIPv1 (1)   ▼ IP Address: 192.10.10.0, Metric: 1     Address Family: IP (2)     IP Address: 192.10.10.0     Metric: 1   ▼ IP Address: 192.20.20.0, Metric: 2     Address Family: IP (2)     IP Address: 192.20.20.0     Metric: 2   ▼ IP Address: 192.30.30.0, Metric: 1     Address Family: IP (2)     IP Address: 192.30.30.0     Metric: 1         </pre>
--	--

Como podemos verificar, o split-horizon faz com que cada interface do router anuncie apenas as redes destino para as quais essa interface não é usada no encaminhamento de pacotes de dados. Este é um mecanismo de prevenção de loops, evitando o congestionamento da rede com pacotes RIP.

Removendo a ligação da interface do router 1 ligada à rede 192.30.30.0, obtemos o seguinte:

```

▶ Frame 466: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface -, id 0
▶ Ethernet II, Src: ca:03:13:c3:00:1c (ca:03:13:c3:00:1c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▶ Internet Protocol Version 4, Src: 192.10.10.2, Dst: 255.255.255.255
▶ User Datagram Protocol, Src Port: 520, Dst Port: 520
▼ Routing Information Protocol
  Command: Response (2)
  Version: RIPv1 (1)
  ▼ IP Address: 192.20.20.0, Metric: 1
    Address Family: IP (2)
    IP Address: 192.20.20.0
    Metric: 1
  ▼ IP Address: 192.30.30.0, Metric: 2
    Address Family: IP (2)
    IP Address: 192.30.30.0
    Metric: 2
    
```

Verifica-se que a informação da rede 192.30.30.0 passa a ser enviada do router 2 para o router 3 e este envia a informação desta rede ao router 1, que já não tem ligação à rede (192.30.30.0) através da interface f1/0. Assim, a rede adaptou-se quando se deparou com um erro na conectividade.

Adicionando a configuração do ex. 6, as tabelas de encaminhamento dos restantes routers obtêm uma linha nova. Exemplo no R3: “R\* 0.0.0.0/0 [120/1] via 192.20.20.2, 00:00:13, FastEthernet0/0”.

O router que aplica este comando vai distribuir uma rota padrão para o protocolo RIP.

## Protocolo OSPF

Configurando todos os routers para suportar o protocolo OSPF, obtemos o seguinte nas tabelas de encaminhamento dos routers. Exemplo do router 1:

```
C 192.30.30.0/24 is directly connected, FastEthernet1/0
C 192.10.10.0/24 is directly connected, FastEthernet0/0
O 192.20.20.0/24 [110/2] via 192.30.30.2, 00:00:04, FastEthernet1/0
  [110/2] via 192.10.10.2, 00:00:04, FastEthernet0/0
```

Usando o comando “show ip ospf interface”:

```
R1#show ip ospf interface
FastEthernet1/0 is up, line protocol is up
  Internet Address 192.30.30.1/24, Area 0
  Process ID 1, Router ID 192.30.30.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.30.30.1, Interface address 192.30.30.1
  Backup Designated router (ID) 192.30.30.2, Interface address 192.30.30.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:02
  Supports Link-local Signaling (LLS)
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.30.30.2 (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
FastEthernet0/0 is up, line protocol is up
  Internet Address 192.10.10.1/24, Area 0
  Process ID 1, Router ID 192.30.30.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.30.30.1, Interface address 192.10.10.1
  Backup Designated router (ID) 192.20.20.1, Interface address 192.10.10.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:05
  Supports Link-local Signaling (LLS)
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.20.20.1 (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
```

Este comando, bem como os restantes do ex.8 permitem saber qual é o DR (Designated Router) de cada uma das redes, além de outras informações igualmente importantes.

Configurando o PC conforme o solicitado no ex. 9, os pacotes ICMP Request passam sempre no sentido inverso dos ponteiros do relógio: de 192.20.20.1 → 192.20.20.2 → 192.30.30.2 (destino). Contudo, o sentido do envio dos pacotes ICMP Reply depende do custo de cada interface.

Por exemplo, se o custo da interface f0/0 do router 1 for 100, este valor é elevado, o que significa que o custo para o ICMP reply ir do router 3 para o PC é mais dispendioso no sentido inverso dos ponteiros do relógio do que no sentido normal dos ponteiros do relógio. Deste modo, se aumentarmos este valor do custo da int f0/0 no router 1 o ICMP reply dirige-se no sentido dos ponteiros do relógio.

No entanto, caso este custo seja 1 (valor reduzido), a passagem do ICMP reply no sentido inverso é mais benéfico do que no sentido normal dos ponteiros do relógio. Assim, se quisermos que o ICMP Request/Reply circule SEMPRE no sentido inverso devemos ter um valor mais reduzido na int f0/0 do router 1.

Os restantes exercícios (RIPng e OSPFv3) são similares aos anteriores, uma vez que a única diferença é que os endereços destes passam a ser IPv6 em vez de IPv4, bem como os endereços de multicasting.