

Dicas de Correção do Exame de Redes e Serviços
20 de Janeiro de 2017

1ª parte

1a)

O switch/bridge raiz é o SW2, porque é o switch com o menor ID (uma das menores prioridades, 6998h, e o menor MAC address de entre os que têm este valor de prioridade).

	Custo para a raiz (RPC)	Porta raiz	Portas designadas	Portas bloqueadas	Justificações
Switch 1	5	2	3	1	A porta 2 é raiz, sendo o RPC de 5. A porta 1 está bloqueada já que o SW6 proporciona melhor caminho para a raiz (igual custo mas menor ID).
Switch 2	0	--	1,2,3,4	--	Switch Raíz
Switch 3	15	3	--	1,2	Portas 1 e 2 estão bloqueadas.
Switch 4	5	2	1,3	--	Portas 1 e 3 são designadas (fornecem menor custo para a raiz).
Switch 5	10	2	--	1,3	Porta 2 é raiz. Portas 1 e 3 estão bloqueadas.
Switch 6	5	3	1,2,4,5	--	
SWL3 A	10	2	1	--	A porta 1 é designada porque fornece o menor custo para a raiz (10) em comparação com a porta 1 do SWL3 B.
SWL3 B	15	2	--	1	A porta 1 está bloqueada porque fornece maior custo para a raiz (15) em comparação com a porta 1 do SWL3 A.

b) Não. Por um lado, falta redundância, porque o SW6 é um ponto único de falha. Deveria ser adicionada uma ligação SW1 → SWL3 A e outra SW3 → SWL3 B, por exemplo. (50%)

Por outro lado, era mais benéfico que o switch raiz fosse o SWL3 A ou B, uma vez que assim minimiza o tráfego na rede de switches. (50%)

1c)

O SW4 avaria, logo deixa de enviar BPDUs para as portas 1 e 3, onde é designado. Ao fim de MAX AGE, os SW3 e SW5 assumem que o SW4 avariou. Nessa altura, o SW5 assume que é designado na LAN que o liga ao SW4, pelo que a sua porta 3 irá passar de *blocking* a *forwarding* (passando pelo estado *learning*). Nesse sentido, envia um TCN-BPDU para a raiz pela porta 2, esta responde com um Conf-BPDU com as flags TCA e TC a "1".

O SW3 irá ativar a sua porta 2, que passará raiz, enquanto que a porta 3 passa a designada. Passa a enviar Conf-BPDUs pela porta designada.

2a)

PÚBLICO:

A VLAN1 precisa de 16 IPv4 públicos, logo a sub-rede deverá ter um tamanho de 16 (12+2 routers+ID+Broadcast=16 → 16); máscara /28.

A VLAN3 precisa de 13 IPv4 públicos, logo a sub-rede deverá ter um tamanho de 16 (9+2 routers+ID+Broadcast=13 → 16); máscara /28.

A rede do DMZ precisa de 14 IPv4 públicos, logo a sub-rede deverá ter um tamanho de 16 (10+2 routers+ID+Broadcast=14 → 16); máscara /28.

O NAT precisa de 10 IPv4 públicos, logo a sub-rede deverá ter um tamanho de 16 (10+ID+Broadcast=12 → 16); máscara /28.

Fazendo subnetting da rede 193.1.1.0/26:

193.136.1.00xx/28, em que xx pode ser 00, 01, 10, 11, obtemos as seguintes subredes:

VLAN1	193.1.1.0/28
VLAN3	193.1.1.16/28
DMZ	193.1.1.32/28
NAT	193.1.1.48/28

PRIVADO:

Todas as LANs precisam de redes privadas (pode-se assumir máscara /24 para todas as (V)LANs e para as ligações ponto-a-ponto Router-Router). Como a rede disponível é 192.168.0.0/16, pode-se usar qualquer IPv4 192.168.X.0/24.

VLAN1	192.168.1.0/24
VLAN2	192.168.2.0/24
VLAN3	192.168.3.0/24
Datacenter	192.168.4.0/24
DMZ	192.168.5.0/24
Rede SWL3A-R4	192.168.6.0/24
Rede SWL3A-R3	192.168.7.0/24
Rede SWL3B-R3	192.168.8.0/24
Rede SWL3B-R2	192.168.9.0/24
Rede R1-R4	192.168.10.0/24
Rede R1-R3	192.168.11.0/24
Rede R2-R3	192.168.12.0/24

2b)

A rede IPv6 disponível é 2100:2100:2100::/60 logo pode-se definir qualquer endereço que comece por 2100:2100:2100:000X::/64 (a máscara fixa os primeiros 60 bits do endereço). Pode-se/deve-se assumir redes com máscara /64.

VLAN1	2100:2100:2100:0000::/64
VLAN2	2100:2100:2100:0001::/64
VLAN3	2100:2100:2100:0002::/64
Datacenter	2100:2100:2100:0003::/64
DMZ	2100:2100:2100:0004::/64
Rede SWL3A-R4	2100:2100:2100:0005::/64
Rede SWL3A-R3	2100:2100:2100:0006::/64
Rede SWL3B-R3	2100:2100:2100:0007::/64
Rede SWL3B-R2	2100:2100:2100:0008::/64
Rede R1-R4	2100:2100:2100:0009::/64
Rede R1-R3	2100:2100:2100:000A::/64
Rede R2-R3	2100:2100:2100:000B::/64

2c)

- Configurar nos switches L2 as portas de acesso para a VLAN 4
- Configurar nos SWL3 A e B a nova VLAN (adicionando-a à base de dados e definindo o interface da nova VLAN), colocando os respectivos endereços IPv4 e IPv6
- Configurar os protocolos RIPng e OSPFv3 no interface VLAN 4 dos SWL3 A e B
- Nos SWL3 A e B adicionar aos protocolos RIPv2 e OSPFv2 a rede correspondente à VLAN 4.

2d)

Em IPv6:

Neste caso, será necessário despoletar o processo de descoberta do endereço MAC do default gateway (endereço VLAN1 do SWL3A). O terminal irá enviar um pacote ICMPv6 Neighbor-Solicitation para o endereço multicast Solicited-Node, tendo como endereço origem o seu endereço IPv6 Global. Receberá como resposta um ICMPv6 Neighbor-Advertisement com o MAC address solicitado. Após esta interação, o terminal irá enviar um ICMPv6 ECHO REQUEST para o endereço Global do interface VLAN1 do SWL3A.

Este swicth irá repetir o mesmo processo para descobrir o MAC do PCB, enviando-lhe o pacote ICMPv6 ECHO REPLY para o seu endereço IPv6 Global. O PCB irá responder com o ICMPv6 ECHO REPLY, via redes de switches, SWL3A, até ao PCA.

Em IPv4:

O PCA terá que descobrir o endereço MAC do default gateway (endereço VLAN1 do SWL3A). O terminal irá enviar um pacote ARP Request para o endereço MAC de broadcast, que ao chegar aos switches L2 sofre flooding até chegar ao interface VLAN1 do SWL3A. Este irá responder com um ARP REPLY. Após esta interação, o terminal irá enviar um ICMP ECHO REQUEST para o interface VLAN1 do SWL3A.

Este switch irá repetir o mesmo processo para descobrir o MAC do PCB, enviando-lhe o pacote ARP Request e recebendo um ARP REPLY. Depois envia o ICMP ECHO REQUEST. O PCB irá responder com o ICMP ECHO REPLY, via redes de switches, SWL3A, até ao PCA.

3. a)

É necessário configurar rotas estáticas nos routers SWL3A, 1 e 2.

Possível solução:

SWL3A:

```
ip route Rede_IPv4_DMZ máscara_Rede_IPv4_DMZ endIPv4_eth1_Router3      ! Next-hop
```

```
ipv6 route Rede_IPv6_DMZ/n°bits_máscara_Rede_IPv6_DMZ endIPv6_eth1_Router3  ! Next-hop
```

Router 1:

```
ip route Rede_IPv4_VLAN1 máscara_Rede_IPv4_VLAN1 endIPv4_eth0_Router3
```

```
ip route Rede_IPv4_VLAN2 máscara_Rede_IPv4_VLAN2 endIPv4_eth0_Router3
```

```
ip route Rede_IPv4_VLAN3 máscara_Rede_IPv4_VLAN3 endIPv4_eth0_Router3
```

```
ip route Rede_IPv4_R4-SWL3A máscara_Rede_IPv4_R4-SWL3A endIPv4_eth0_Router3
```

```
ip route Rede_IPv4_R3-SWL3A máscara_Rede_IPv4_R3-SWL3A endIPv4_eth0_Router3
```

```
ipv6 route Rede_IPv6_VLAN1/n°bits_máscara_Rede_IPv6_VLAN1 endIPv6_eth0_Router3
```

```
ipv6 route Rede_IPv6_VLAN2/n°bits_máscara_Rede_IPv6_VLAN2 endIPv6_eth0_Router3
```

```
ipv6 route Rede_IPv6_VLAN3/n°bits_máscara_Rede_IPv6_VLAN3 endIPv6_eth0_Router3
```

```
ipv6 route Rede_IPv6_R4-SWL3A/n°bits_máscara_Rede_IPv6_R4-SWL3A endIPv6_eth0_Router3
```

```
ipv6 route Rede_IPv6_R3-SWL3A/n°bits_máscara_Rede_IPv6_R3-SWL3A endIPv6_eth0_Router3
```

Router 2:

```
ip route Rede_IPv4_VLAN1 máscara_Rede_IPv4_VLAN1 endIPv4_eth3_Router3
```

```
ip route Rede_IPv4_VLAN2 máscara_Rede_IPv4_VLAN2 endIPv4_eth3_Router3
```

```
ip route Rede_IPv4_VLAN3 máscara_Rede_IPv4_VLAN3 endIPv4_eth3_Router3
```

```
ip route Rede_IPv4_R4-SWL3A máscara_Rede_IPv4_R4-SWL3A endIPv4_eth3_Router3
```

```
ip route Rede_IPv4_R3-SWL3A máscara_Rede_IPv4_R3-SWL3A endIPv4_eth3_Router3
```

```
ipv6 route Rede_IPv6_VLAN1/n°bits_máscara_Rede_IPv6_VLAN1 endIPv6_eth3_Router3
```

```
ipv6 route Rede_IPv6_VLAN2/n°bits_máscara_Rede_IPv6_VLAN2 endIPv6_eth3_Router3
```

```
ipv6 route Rede_IPv6_VLAN3/n°bits_máscara_Rede_IPv6_VLAN3 endIPv6_eth3_Router3
```

```
ipv6 route Rede_IPv6_R4-SWL3A/n°bits_máscara_Rede_IPv6_R4-SWL3A endIPv6_eth3_Router3
```

```
ipv6 route Rede_IPv6_R3-SWL3A/n°bits_máscara_Rede_IPv6_R3-SWL3A endIPv6_eth3_Router3
```

3b)

O PCA terá que descobrir o endereço MAC do default gateway (endereço VLAN1 do SWL3A). O terminal irá enviar um pacote ARP Request para o endereço MAC de broadcast, que ao chegar aos switches L2 sofre flooding até chegar ao interface VLAN1 do SWL3A. Este irá responder com um ARP REPLY. Após esta interação, o terminal irá enviar um ICMP ECHO REQUEST para o interface VLAN1 do SWL3A.

Este switch irá repetir o mesmo processo para descobrir o MAC do next hop (o interface eth1 do Router 3, enviando-lhe o pacote ARP Request e recebendo um ARP REPLY. Depois envia o ICMP ECHO REQUEST. O Router 3 repetirá o mesmo processo para finalmente atingir o Router 2.

A resposta será encaminhada para o Router 3 e daí para o SWL3A.

Parte 2

1a)

As tabelas de encaminhamento têm de possuir: Protocolo, rede e máscara, custo até ao destino, endereço IP do next-hop (próximo router) e interface de saída (layer 3 e não número de portas layer 2!).

Tabela de encaminhamento SWL3A

```
C    redeVLAN1, diretamente ligada, interface vlan1
C    redeVLAN2, diretamente ligada, interface vlan2
C    redeVLAN3, diretamente ligada, interface vlan2
C    redeR4-SWL3A, diretamente ligada, interface eth0
C    redeR3-SWL3A, diretamente ligada, interface eth1
---
O    redeR3-SWL3B, [custo 15] via endIP_intVLAN1_SWL3B, interface vlan1
                                via endIP_intVLAN2_SWL3B, interface vlan2
                                via endIP_intVLAN3_SWL3B, interface vlan3
                                via endIP_eth1R3, interface eth1
O    redeR2-SWL3B, [custo 10] via endIP_intVLAN1_SWL3B, interface vlan1
                                via endIP_intVLAN2_SWL3B, interface vlan2
                                via endIP_intVLAN3_SWL3B, interface vlan3
O    redeR2-R3, [custo 20] via endIP_intVLAN1_SWL3B, interface vlan1
                                via endIP_intVLAN2_SWL3B, interface vlan2
                                via endIP_intVLAN3_SWL3B, interface vlan3
O    redeR1-R3, [custo 15] via endIP_eth1R3, interface eth1
O    redeR1-R4, [custo 20] via endIP_eth2R4, interface eth0
O    rede Datacenter, [custo 30] via endIP_eth2R4, eth0
O    rede DMZ, [custo 20] via endIP_intVLAN1_SWL3B, interface vlan1
                                via endIP_intVLAN2_SWL3B, interface vlan2
                                via endIP_intVLAN3_SWL3B, interface vlan3
---
```

(rotas por omissão obtidas por OPSF, vamos assumir tipo E2, custos iguais por qualquer caminho)

```
IPv4 → O 0.0.0.0/0, [custo 20] via endIP_intVLAN1_SWL3B, interface vlan1
                                via endIP_intVLAN2_SWL3B, interface vlan2
                                via endIP_intVLAN3_SWL3B, interface vlan3
                                via endIP_eth2R4, interface eth0
                                via endIP_eth1R3, interface eth1
IPv6 → O ::/0, [custo 20] via endIP_intVLAN1_SWL3B, interface vlan1
                                via endIP_intVLAN2_SWL3B, interface vlan2
                                via endIP_intVLAN3_SWL3B, interface vlan3
                                via endIP_eth2R4, interface eth0
                                via endIP_eth1R3, interface eth1
```

1b)

Para garantir os requisitos é preciso alterar os custos do OSPF de modo a garantir que este caminho tenha o menor custo de todos os caminhos possíveis.

Possível solução:

Diminuir o custo dos interfaces eth1 do SWL3A para 1, do interface eth1 do Router 3 para 1 e do interface eth3 do Router 1 para 1. Assim o custo do caminho SWL3A/B → Router 3 → Router 1 → Router 4 → Datacenter fica igual a 23, menor que qualquer outro caminho.

1c)

Tabela de encaminhamento SWL3B

C	redeVLAN1, diretamente ligada, interface vlan1
C	redeVLAN2, diretamente ligada, interface vlan2
C	redeVLAN3, diretamente ligada, interface vlan2
C	redeR3-SWL3B, diretamente ligada, interface eth1
C	redeR2-SWL3B, diretamente ligada, interface eth0

O	redeR3-SWL3A, [custo 15] via endIP_intVLAN1_SWL3A, interface vlan1 via endIP_intVLAN2_SWL3A, interface vlan2 via endIP_intVLAN3_SWL3A, interface vlan3
O	redeR4-SWL3A, [custo 15] via endIP_intVLAN1_SWL3A, interface vlan1 via endIP_intVLAN2_SWL3A, interface vlan2 via endIP_intVLAN3_SWL3A, interface vlan3
O	redeR2-R3, [custo 30] via endIP_eth2Router3, interface eth1
O	redeR1-R3, [custo 15] via endIP_eth2R3, interface eth1
O	redeR1-R4, [custo 25] via endIP_intVLAN1_SWL3A, interface vlan1 via endIP_intVLAN2_SWL3A, interface vlan2 via endIP_intVLAN3_SWL3A, interface vlan3
O	rede Datacenter, [custo 35] via endIP_intVLAN1_SWL3A, interface vlan1 via endIP_intVLAN2_SWL3A, interface vlan2 via endIP_intVLAN3_SWL3A, interface vlan3
R	rede DMZ, [120/custo 2] via endIP_eth3Router2, interface eth0

(rotas por omissão obtidas por OPSF, vamos assumir tipo E2, custos iguais por qualquer caminho)

IPv4 → R 0.0.0.0/0, [120/custo 3] via endIP_intVLAN1_SWL3A, interface vlan1
via endIP_intVLAN2_SWL3A, interface vlan2
via endIP_intVLAN3_SWL3A, interface vlan3
via endIP_eth2Router3, interface eth1
via endIP_eth3Router2, interface eth0

IPv6 → R ::/0, [120/custo 3] via endIP_intVLAN1_SWL3A, interface vlan1
via endIP_intVLAN2_SWL3A, interface vlan2
via endIP_intVLAN3_SWL3A, interface vlan3
via endIP_eth2Router3, interface eth1
via endIP_eth3Router2, interface eth0

2. a)

C 210.2.2.0/26, directly connected, eth1
C 100.0.0.0/30, directly connected, eth0
B 210.1.1.0/27 [20/0], via 100.0.0.1, eth0
B 193.1.1.0/26 [20/0], via 100.0.0.1, eth0

b)

Se o interface eth1 for desligado, o Router B irá enviar BGP Update para notificar da perda dessa rede. Esses pacotes serão enviados para o Router 1, que por sua vez irá enviar um BGP Update para o Router A. Para além disso, os routers BGP trocam pacotes KEEPALIVE para manter as sessões TCP abertas.

3)

Colocaria na interface eth1 do Router 4, sentido de saída, uma ACL standard que permitiria todo o tráfego dos IPs das VLANs 1, 2 e 3 e negaria todo o restante tráfego.

```
access-list 1 permit IP_VLAN1
```

```
access-list 1 permit IP_VLAN2
```

```
access-list 1 permit IP_VLAN3
```

4)

UDP, porto destino 80 →

PORTO UDP 80 ESTÁ FECHADO!

←ICMP PORT UNREACHABLE (port 80)

5)

Os cookies são uma forma do servidor identificar um terminal em diferentes pedidos feitos no tempo. Permite ao servidor diferenciar a informação a disponibilizar por terminal.

A primeira vez que um terminal enviar um request a um servidor, o servidor inclui na resposta uma linha de cabeçalho. Se o browser for configurado para aceitar cookies, ele guarda este número juntamente com o identificador do servidor. Em futuros pedidos, o browser inclui a linha de cabeçalho. Deste modo, o servidor identifica o terminal.

6)

Em IPv4, o gateway de cada rede local deverá ser configurado como “BootP Relay Agent”. O router irá redirecionar todos os pacotes DHCP (recebidos em broadcast) para o servidor DHCP usando unicast. Adiciona informação na mensagem com a indicação da rede/interface onde recebeu o pedido. As respostas do servidor são reenviadas para o cliente.

O mecanismo de relay em DHCPv6 funciona de forma distinta do que no DHCP para IPv4.

O Relay Agent encapsula completamente as mensagens DHCPv6 do cliente numa nova mensagem do tipo RELAY-FORW message.

Reencaminha esta nova mensagem para o servidor de DHCPv6.

A resposta é feita igualmente usando uma nova mensagem (RELAY-REPL message) que contém encapsulada a mensagem a enviar ao cliente DHCPv6 pelo Relay Agent.

7)

```
NS      ns1.maisvalor.pt
MX      10    mail1.maisvalor.pt
```

```
ns1     A      endIPv4_DNS
ns1     AAAA   endIPv6_DNS
mail1   A      endIPv4_mail1
mail1   AAAA   endIPv6_mail1
http1   A      endIPv4_http1
http1   AAAA   endIPv6_http1
http2   A      endIPv4_http2
http2   AAAA   endIPv6_http2
```

```
maisvalor.pt      CNAME    http1
www.maisvalor.pt  CNAME    http2
```