

Dicas de Correção do Exame de Redes e Serviços
16 de Janeiro de 2018

1a)

O switch/bridge raiz é o SW4, porque é o switch com o menor ID (a menor prioridade, 6998h).

	Custo para a raiz (RPC)	Porta raiz	Portas designadas	Portas bloqueadas	Justificações
Switch 1	15	2	--	1,3	A porta 2 é raiz, sendo o RPC de 15. A porta 1 está bloqueada já que o SW3A proporciona melhor caminho para a raiz (igual custo mas menor ID). A porta 3 está bloqueada já que o SW5 proporciona melhor caminho para a raiz (menor custo).
Switch 2	10	4	1,2,4,5,6	3	A porta 3 está bloqueada já que o SW5 proporciona melhor caminho para a raiz (menor custo).
Switch 3	10	3	1	2	A porta 2 está bloqueada já que o SW2 proporciona melhor caminho para a raiz (igual custo mas o ID do SW2 é menor).
Switch 4	0	--	1,2,3	--	Switch raiz.
Switch 5	5	3	1,2	--	Porta 3 é raiz. Portas 1 e 2 são designadas já que oferecem o menor custo para a raiz.
SWL3 A	15	2	1	--	A porta 1 é designada porque fornece o menor custo para a raiz em comparação com a porta 1 do SW1 (igual custo mas menor ID).
SWL3 B	15	1	--	2	A porta 2 está bloqueada porque fornece maior custo para a raiz (15) em comparação com a porta 1 do SW3.

b) Era mais benéfico que o switch raiz fosse o SWL3 A ou B, uma vez que assim minimizaria o tráfego na rede de switches sempre que a comunicação seja feita de e para a Internet, DMZ ou Datacenter. Para conseguir esse objetivo, deveria diminuir a prioridade do SWL3A ou B para um valor inferior a 6998h, por exemplo 6997h.

1c)

O SW5 avaria, logo deixa de enviar Configuration BPDUs para as portas 1 e 2, onde é designado. Ao fim de MAX AGE, os SW1 e SW2 assumem que o SW5 avariou.

Nessa altura, o SW1 assume que é designado na LAN que o liga ao SW5, pelo que a sua porta 3 irá passar do estado *blocking* ao estado *forwarding* (passando pelos estados intermédios *learning* e *listening*). Nesse sentido, o SW1 envia um TCN-BPDU em direção à raiz pela porta 2 (porta raiz), esta responde com um Conf-BPDU com as flags TCA e TC a "1" para o SW2, que por sua vez enviará um Conf-BPDU com as flags TCA e TC a "1" para o SW1.

Da mesma forma, o SW2 assume que é designado na LAN que o liga ao SW5, pelo que a sua porta 3 irá passar de *blocking* a *forwarding* (passando pelos estados *learning* e *listening*). Nesse sentido, envia um TCN-BPDU para a raiz pela porta 4 (porta raiz), esta responde com um Conf-BPDU com as flags TCA e TC a "1".

2a)

PÚBLICO:

A VLAN1 precisa de 18 IPv4 públicos, logo a sub-rede deverá ter um tamanho de 32 ($18+2 \text{ routers}+ID+Broadcast=22 \rightarrow 32$); máscara /27.

A VLAN2 precisa de 14 IPv4 públicos, logo a sub-rede deverá ter um tamanho de 32 ($14+2 \text{ routers}+ID+Broadcast=18 \rightarrow 32$); máscara /27.

A rede do DC precisa de 12 IPv4 públicos, logo a sub-rede deverá ter um tamanho de 16 ($12+2 \text{ routers}+ID+Broadcast=16 \rightarrow 16$); máscara /28.

A rede do DMZ precisa de 4 IPv4 públicos, logo a sub-rede deverá ter um tamanho de 8 ($4+2 \text{ routers}+ID+Broadcast=8 \rightarrow 8$); máscara /29.

O NAT precisa de 5 IPv4 públicos, logo a sub-rede deverá ter um tamanho de 8 ($5+ID+Broadcast=7 \rightarrow 8$); máscara /29.

Fazendo subnetting da rede 194.1.1.0/25:

194.1.1.0xx/27, em que xx pode ser 00, 01, 10, 11, obtemos as seguintes subredes:

VLAN1	194.1.1.0/27
VLAN2	194.1.1.32/27
	194.1.1.64/27
	194.1.1.96/27

Fazendo subnetting da rede seguinte:

194.1.1.010X/28, em que X pode ser 0 ou 1, obtemos as seguintes subredes:

DC	194.1.1.64/28
	194.1.1.80/28

Fazendo subnetting da rede seguinte:

194.1.1.0101X/29, em que X pode ser 0 ou 1, obtemos as seguintes subredes:

DMZ	194.1.1.80/29
NAT/PAT	194.1.1.88/29

A subrede 194.1.1.96/27 fica livre.

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-SWL3B	192.168.6.0/24
Rede SWL3A-R2	192.168.7.0/24
Rede SWL3B-R2	192.168.8.0/24
Rede SWL3B-SWL3C	192.168.9.0/24
Rede R2-SWL3C	192.168.10.0/24

A rede IPv6 disponível é 2100:10:10::/60 logo pode-se definir qualquer endereço que comece por 2100:10:10:000X::/64 (a máscara fixa os primeiros 60 bits do endereço). Pode-se/deve-se assumir redes com máscara /64.

VLAN1	2100:10:10:0000::/64
VLAN2	2100:10:10:0001::/64
VLAN3	2100:10:10:0002::/64
Datacenter	2100:10:10:0003::/64
DMZ	2100:10:10:0004::/64
Rede SWL3A-SWL3B	2100:10:10:0005::/64
Rede SWL3A-R2	2100:10:10:0006::/64
Rede SWL3B-R2	2100:10:10:0007::/64
Rede SWL3B-SWL3C	2100:10:10:0008::/64
Rede R2-SWL3C	2100:10:10:0009::/64

2b)

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, SW4, SW2 e SW1 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 PC C (localizado na VLAN 3), 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, SW4, SW2 e SW1 até ao PCA.

3. a)

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	SWL3A-SWL3B, diretamente ligada, interface eth1
C	redeR2-SWL3A, diretamente ligada, interface eth0
R	redeR2-SWL3B, [120/custo 1] via endIP_VLAN1_SWL3B, interface vlan1 via endIP_VLAN2_SWL3B, interface vlan2 via endIP_VLAN3_SWL3B, interface vlan3 via endIP_eth2_SWL3B, eth1 via endIP_eth4_R2, eth0
R	redeSWL3B-SWL3C, [120/custo 1] via endIP_VLAN1_SWL3B, interface vlan1 via endIP_VLAN2_SWL3B, interface vlan2 via endIP_VLAN3_SWL3B, interface vlan3 via endIP_eth2_SWL3B, interface eth1
R	redeR2-SWL3C, [120/custo 1] via endIP_eth4R2, interface eth0
R	redeDMZ, [120/custo 1] via endIP_eth4R2, interface eth0
R	redeDC, [120/custo 2] via endIP_VLAN1_SWL3B, interface vlan1 via endIP_VLAN2_SWL3B, interface vlan2 via endIP_VLAN3_SWL3B, interface vlan3 via endIP_eth2_SWL3B interface eth1 via endIP_eth4_R2, interface eth0

(rota por omissão obtida por RIP)

R 0.0.0.0/0, [120/custo 1] via endIP_eth4R2, interface eth0

b)

Tabela de encaminhamento SWL3A

C	redeVLAN1, diretamente ligada, interface vlan1
C	redeVLAN2, diretamente ligada, interface vlan2
C	redeVLAN3, diretamente ligada, interface vlan2
C	SWL3A-SWL3B, diretamente ligada, interface eth1
C	redeR2-SWL3A, diretamente ligada, interface eth0
O	redeR2-SWL3B, [110/custo 10] via endIP_VLAN1_SWL3B, interface vlan1 via endIP_VLAN2_SWL3B, interface vlan2 via endIP_VLAN3_SWL3B, interface vlan3
O	redeSWL3B-SWL3C, [110/custo 10] via endIP_VLAN1_SWL3B, interface vlan1 via endIP_VLAN2_SWL3B, interface vlan2 via endIP_VLAN3_SWL3B, interface vlan3
O	redeR2-SWL3C, [110/custo 20] via endIP_VLAN1_SWL3B, interface vlan1 via endIP_VLAN2_SWL3B, interface vlan2

via endIP_VLAN3_SWL3B, interface vlan3
via endIP_eth4R2, interface eth0

O redeDMZ, [110/custo 15] via endIP_VLAN1_SWL3B, interface vlan1
via endIP_VLAN2_SWL3B, interface vlan2
via endIP_VLAN3_SWL3B, interface vlan3
via endIP_eth4R2, interface eth0

O redeDC, [110/custo 25] via endIP_VLAN1_SWL3B, interface vlan1
via endIP_VLAN2_SWL3B, interface vlan2
via endIP_VLAN3_SWL3B, interface vlan3
via endIP_eth4_R2, interface eth0

(rota por omissão obtida por OSPFv3)

O ::/0, [110/custo 20] via endIP_VLAN1_SWL3B, interface vlan1
via endIP_VLAN2_SWL3B, interface vlan2
via endIP_VLAN3_SWL3B, interface vlan3
via endIP_eth4R2, interface eth0
via endIP_eth2_SWL3B, interface eth1

c)

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:

Caminho a partir do SWL3A:

Aumentar o custo da interface eth1 do SWL3B para 20, do interface eth1 do Router 2 para 20 e diminuir o custo do interface eth0 do SWL3C para 1. Assim o custo do caminho SWL3A → SWL3B → SWL3C → Datacenter fica igual a 11, saindo pela interfaces VLAN.

Caminho a partir do SWL3B:

Com estes custos, o custo do caminho SWL3B → SWL3C → Datacenter fica igual a 6, o menor de todos os caminhos possíveis.

4. a)

C 210.1.1.0/27, directly connected, eth1

C 100.0.0.0/29, directly connected, eth0

B 194.1.1.0/25 [20/0], via 100.0.0.1, eth0
via 100.0.0.2, eth0

b)

Nenhuma mensagem nova, os routers continuarão a trocar pacotes KEEPALIVE para manter as sessões TCP abertas. Note-se que o Router 2 está a anunciar o agregado das redes IP do SA 1111, logo uma alteração de uma das redes do agregado não implica a troca de qualquer mensagem BGP Update.

c)

Poderíamos configurar o atributo Local Preference nos routers 1 e 2, colocando um valor mais elevado no Router 1.

d)

Poderíamos configurar o atributo Multi-Exit Discriminator nos routers 1 e 2, colocando um valor mais baixo no Router 2. Este atributo é usado como sugestão a dar ao SA 2222.

5)

(i) Colocaria nas interfaces eth0 dos Routers 1 e 2, sentido de entrada, uma **ACL estendida** que impediria o protocolo ICMP com destino à rede IP pública do SA 1111:

```
access-list 100 deny ICMP any 194.1.1.0 255.255.255.128
access-list 100 permit any any
```

(ii) Colocaria nas interfaces ethernet de saída dos SWL3A (eth0, eth1, vlan1, vlan2, vlan3) e SWL3B (eth0, eth1, vlan1, vlan2, vlan3) uma **ACL estendida** que impedisse todo o tráfego proveniente da VLAN 1 e destinado à DMZ:

```
access-list 101 deny ip IPprivado_VLAN1 IPprivado_DMZ
access-list 101 deny ip IPprivado_VLAN1 IPpúblico_DMZ
access-list 101 deny ip IPpúblico_VLAN1 IPprivado_DMZ
access-list 101 deny ip IPpúblico_VLAN1 IPpúblico_DMZ
access-list 101 deny ip IPv6_VLAN1 IPv6_DMZ
access-list 101 permit any any
```