Dicas de Correção do Exame de Recurso de Redes e Serviços
24 de fevereiro de 2022

1a)

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

	Custo para a raiz (RPC)	Porta raiz	Portas designadas	Portas bloqueadas	Justificações
Switch 1	15	2	--	1,3	
Switch 2	10	4	1,2,5,6	3	A porta 2 está bloqueada, porque embora proporcione um custo de 5 para a raiz, tal como a porta 2 do SW1, o ID do SW1 é menor.
Switch 3	10	3	1	2	A porta 2 está bloqueada, porque embora proporcione um custo de 10 para a raiz, tal como a porta 5 do SW2, o ID do SW2 é menor.
Switch 4	0	--	1,2,3	--	ROOT
Switch 5	5	3	1,2	--	
SWL3 A	15	2	1	--	
SWL3 B	15	1	--	2	

b)

MAC Address	**Port**
MAC_PC 1	4
MAC_PC 2	2
MAC_PC 3	2
MAC Default gateway VLAN 1	2

2a)
PÚBLICO:

A VLAN 1 precisa de 20 IPv4 públicos, logo a sub-rede deverá ter um tamanho de 32 (20+2 routers+ID+Broadast=24 → 32); máscara /27.

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

A rede do DC precisa de 6 IPv4 públicos, logo a sub-rede deverá ter um tamanho de 16 (6+2 routers+ID+Broadast=10 → 16); máscara /28.

A rede do DMZ precisa de 6 IPv4 públicos, logo a sub-rede deverá ter um tamanho de 16 (6+2 routers+ID+Broadast=10 → 16); máscara /28.

O NAT precisa de 4 IPv4 públicos, logo a sub-rede deverá ter um tamanho de 8 (4+ID+Broadast=6 → 8); máscara /29.

Fazendo subnetting da rede 193.20.20.128/25:

193.20.20.1xx/27, em que xx pode ser 00, 01, 10 ou 11, obtemos as seguintes subredes:

VLAN1	193.20.20.128/27
	193.20.20.160/27
	193.20.20.192/27
	193.20.20.224/27

Fazendo subnetting da rede seguinte:

193.20.20.101x/28, em que x pode ser 0 ou 1, obtemos as seguintes subredes:

VLAN2	193.20.20.160/28
DC	193.20.20.176/28

Fazendo subnetting da rede seguinte (193.20.20.192/27):

193.20.20.110x/28, em que x pode ser 0 ou 1, obtemos as seguintes subredes:

DMZ	193.20.20.192/28
	193.20.20.208/28

Fazendo subnetting da rede seguinte (193.20.20.208/28):

193.20.20.1101x/29, em que x pode ser 0 ou 1, obtemos as seguintes subredes:

NAT/PAT	193.20.20.208/29
LIVRE	193.20.20.216/29

A subrede 193.20.20.224/27 também 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 R2-SWL3A	192.168.6.0/24
Rede SWL3B-R2	192.168.7.0/24

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

A rede IPv6 disponível é 3000: 3000: 3000::/60 logo pode-se definir qualquer endereço que comece por 3000: 3000: 3000:000X::/64 (a máscara fixa os primeiros 60 bits do endereço). Pode-se/deve-se assumir redes com máscara /64.

VLAN1	3000:3000:3000:0::/64
VLAN2	3000:3000:3000:1::/64
VLAN3	3000:3000:3000:2::/64
Datacenter	3000:3000:3000:3::/64
DMZ	3000:3000:3000:4::/64
Rede R2-SWL3A	3000:3000:3000:5::/64
Rede SWL3B-R2	3000:3000:3000:6::/64
Rede SWL3C-R2	3000:3000:3000:7::/64
Rede SWL3A-SWL3B	3000:3000:3000:8::/64
Rede SWL3B-SWL3C	3000:3000:3000:9::/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 (percurso SW1 → SW2 → SWL3A).
Este switch irá repetir o mesmo processo para descobrir o MAC do PCB, emviando-lhe o pacote ICMPv6 ECHO REQUEST para o seu endereço IPv6 Global (percurso SWL3A → SW2 → SW4 → SW5 → PCB). O PCB irá responder com o ICMPv6 ECHO REPLY, via redes de switches, SW5 → SW2 → SW1 até ao PCA.

Em IPv4:
O PCB 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 (percurso SW1 → SW2 → SWL3A) .
Este switch irá repetir o mesmo processo para descobrir o MAC do PC B (localizado na VLAN 2), 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, SW5 → SW2 → SW1 até ao PCA.

2c)
Os terminais IPv6 podem obter os seus endereços por **configuração estática** ou **de forma automática** recorrendo a um servidor **DHCPv6 (configuração stateful)** ou **adicionando o identificador do interface (de 64 bits) aos prefixos (de 64 bits) incluídos nas mensagens Router Advertisement (stateless)**.

2d)
Deveria configurar nos routers de saída (R1 e R2) **NAT/PAT estático** em que associava um endereço público da pool do NAT ao endereço privado do servidor (podia também incluir o número de porto).

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 vlan3
C redeSWL3A-Router2, diretamente ligada, interface eth0
C redeSWL3A-SWL3B, diretamente ligada, interface eth1

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 redeDMZ, [110/custo 15] via endIP_VLAN1_SWL3B, interface vlan1
via endIP_VLAN2_SWL3B, interface vlan2
via endIP_VLAN3_SWL3B, interface vlan3
via endIP_eth4R1, interface eth0

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_eth4R1, 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_eth4R1, interface eth0

(rota por omissão obtida por OSPF)
OE2 0.0.0.0/0, [110/custo 10] 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_eth4R1, interface eth0

b)
Há várias hipóteses de garantir esse requisito:
- manter as rotas por omissão com o tipo E2 e fazer com que o Router 1 anuncie uma métrica inferior
- alterar as rotas por omissão para o tipo E1 e alterar os custos do OSPF de modo a garantir que o caminho pelo Router 1 tenha o menor custo. Possível solução: Aumentar o custo das interfaces eth0 do SWL3A, eth1 do SWL3B e eth1 do SWL3C para 50.
.

4. a)
C 210.1.1.0/27, directly connected, eth1
C 100.0.0.0/29, directly connected, eth0
B 193.20.20.128/25 [20/0], via 100.0.0.1, eth0
via 100.0.0.2, eth0

b)
Devemos configurar nos routers 1 e 2 o atributo MED, colocando um valor mais baixo no Router 2. Este atributo influencia o tráfego de entrada.

5)
Políticas de escalonamento – estas políticas decidem a ordem pela qual as diferentes filas de espera e os diferentes pacotes são servidor num sistema (router ou switch). Influenciam sobretudo o atraso sofrido pelos pacotes (atraso na fila de espera).

Descarte de pacotes - estas políticas decidem a ordem pela qual os pacotes são descartados nas filas de espera quando estas atingem um tamanho igual ou superior ao threshold definido. Influenciam sobretudo a taxa de perda de pacotes de cada fluxo.

6)
A transmissão de segmentos TCP é restringida por awnd = min(credit, cwnd)
O procedimento Slow Start de uma nova ligação TCP consiste em:
– é feito cwnd = MSS(Maximum Segment Size);
– para que o atraso até ser atingida uma taxa de transmissão razoável não seja muito elevado, o TCP aumenta a janela mais rapidamente nesta fase
– neste procedimento, cwnd cresce exponencialmente.

Gestão de janelas quando ocorre um timeout (algoritmo de Jacobson):
– Colocar o limiar de slow start ssthresh (slow start threshold) igual a metade da janela actual:
ssthresh = awnd/2
– Fazer cwnd = MSS
– Efectuar o procedimento slow start até que cwnd = ssthresh. Nesta fase, awnd é incrementada de MSS de cada vez que é recebido um ACK.
– Para cwnd ≥ ssthresh, incrementar cwnd linearmente, isto é, incrementar cwnd de MSS em cada RTT.