Correção – Parte 1

1a)

O switch/bridge raiz é o Switch2 porque é o switch com o menor ID (menor prioridade 6998h).

	Custo para a raiz (RPC)	Porta raiz	Portas bloqueadas	Justificações
Switch 1	5	1	-	Ligação direta à raiz. A porta 1 é raiz; as portas 3 e 4 fornecem igual RPC mas o ID do switch 1 é menor do que os ID dos switches SWL3A e SW6; a porta 2 fornece um menor RPC em relação ao SW5, logo são todas designadas.
Switch 2	-	-	-	É o switch raíz
Switch 3	15 (10+5)	4	1,2,3	A porta 3 tem custo igual no caminho via SWL3B e no caminho via SW4. Prefere vizinho com menor ID (SW4).
Switch 4	15 (10+5)	3	2	Porta 3 é a porta raíz (embora o custo seja igual ao da porta 1, o ID do switch 6 é menor);
Switch 5	10 (5+5)	3	1	Porta 3 é raiz, porta 2 é designada (fornece melhor caminho para a raiz em relação ao SW4); porta 1 está bloqueada porque a porta 2 do switch 1 fornece um RPC menor.
Switch 6	5	1	2	A porta 2 está bloqueada porque a porta 3 do switch 1 fornece um caminho melhor (mesmo RPC mas o ID do switch 1 é menor).
SWL3 A	5	1	2	A porta 2 está bloqueada porque a porta 4 do switch 1 fornece um caminho melhor (mesmo RPC mas o ID do switch 1 é menor).
SWL3 B	5	1	-	

1b) Poderia diminuir a prioridade do SWL3A para 6998h, por exemplo.

(Alterações a negrito)

	Custo para a raiz (RPC)	Porta raiz	Portas bloqueadas	Justificações
Switch 1	**10**	**4**	**1**	As portas 2 e 3 são designadas.
Switch 2	**5**	**5**	-	As portas 1, 2, 3 e 4 são designadas.
Switch 3	**20 (10+5+5)**	4	1,2,3	A porta 3 tem custo igual no caminho via SWL3B e no caminho via SW4. Prefere vizinho com menor ID (SW4).
Switch 4	**20 (10+5+5)**	3	2	Porta 3 é a porta raíz (embora o custo seja igual ao da porta 1, o ID do switch 6 é menor);
Switch 5	15 (5+5+5)	3	1	Porta 3 é raiz, porta 2 é designada (fornece melhor caminho para a raiz em relação ao SW4); porta 1 está bloqueada porque a porta 2 do switch 1 fornece um RPC menor.
Switch 6	**10 (5+5)**	1	**-**	A porta 2 está bloqueada porque a porta 3 do

				switch 1 fornece um caminho melhor (mesmo RPC mas o ID do switch 1 é menor).
SWL3 A	-	-	-	-
SWL3 B	**10 (5+5)**	1	-	A porta 2 e designada.

1c)
Tabela de encaminhamento Layer 2 (forwarding table) do SW6

Endereço MAC	Porta (do próprio switch)
MAC_terminalA	4
MAC_terminalB	1
MAC_SW1	2 (MAC aprendido com os pacotes da Spanning-tree)
MAC_SW2	1 (MAC aprendido com os pacotes da Spanning-tree)
MAC_SW3	5 (MAC aprendido com os pacotes da Spanning-tree)
MAC_SW4	4 (MAC aprendido com os pacotes da Spanning-tree)
MAC_SW5	3 (MAC aprendido com os pacotes da Spanning-tree)
MAC_SWL3A	1 (MAC aprendido com os pacotes da Spanning-tree)
MAC_SWL3B	1 (MAC aprendido com os pacotes da Spanning-tree)

2ª) e 2b)

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

A rede do DMZ precisa de 25 IPv4 públicos, logo a sub-rede deverá ter um tamanho de 32 (25+2 routers+ID+Broadast=29 → 32); máscara /27.

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

Começando da rede maior e a partir de 193.11.11.64/26:

DMZ	193.11.11.64/27	(+32 endereços)
VLAN1	193.11.11.96/28	(+16 endereços)
NAT	193.11.11.112/28	(+16 endereços)

Todas as LAN precisam de redes privadas (pode-se assumir máscara /24 para as LANs e /30 para a ligações Router-Router). Como a rede disponível é 192168.0.0/16, pode-se usar qualquer IPv4 192.168.X.X. Logo as LANs podem ter a rede 192.168.X.0/24 com X de 0 a 255.

A rede IPv6 disponível é 2200:A:A:AAA::/60 logo pode-se definir qualquer endereço que comece por 2200:A:A:AAAX:XXXX:XXXX:XXXX:XXXX (a máscara fixa os primeiros 60 bits do endereço). Pode-se/deve-se assumir redes com máscara /64. Logo as LANs podem ter a rede 2200:A:A:AAAX::/64 com X de 0 a F.

Possível solução:

VLAN1	192.168.1.0/24	2200:A:A:AAA1::/64
VLAN2	192.168.2.0/24	2200:A:A:AAA2::/64
VLAN3	192.168.3.0/24	2200:A:A:AAA3::/64
DMZ	192.168.200.0/24	2200:A:A:AAA0::/64
Rede SWA-SWB	192.168.100.0/30	2200:A:A:AAA4::/64
Rede R1-SWA	192.168.100.4/30	2200:A:A:AAA5::/64
Rede R1-SWB	192.168.100.8/30	2200:A:A:AAA6::/64
Rede R1-R2	192.168.100.12/30	2200:A:A:AAA7::/64
Rede R2-SWA	192.168.100.16/30	2200:A:A:AAA8::/64
Rede R2-SWB	192.168.100.20/30	2200:A:A:AAA9::/64

2c)
Como o servidor de DHCP está na DMZ então todos os routers/SWL3 vão ter de redirecionar os pedidos para o servidor (servindo de intermediários). Para esse efeito é preciso configurar todos os routers como BOOTP Relay Agents.
Um terminal que deseje obter um endereço IP irá enviar um pacote DHCP DISCOVER em broadcast, que chegará a um router o qual incluirá no pacote o endereço IPv4 onde recebeu o pacote (para o servidor DHCP poder identificar a rede de origem) e reenviará em unicast o DISCOVER para o servidor, o servidor perante este pedido identifica a rede de origem e procurará na gama de endereços dessa rede um disponível, reenviará a oferta num pacote DHCP OFFER já com o endereço via routers para o terminal, o terminal responderá com um DHCP REQUEST ao qual o servidor (se tudo estiver de acordo com o oferecido) enviará um DHCP ACKNOWLEDGEMENT.

2d) Os endereços IPv6 são constituídos por um prefixo de rede e um interface ID. Nos endereços Link-Local o prefixo de rede é pré-definido (FE80/10) e este endereço é construido após a inicialização do terminal. O terminal envia um pacote ICMPv6 Neighbor Solicitation para verificar se existem endereços duplicados. O terminal envia também um pacote ICMPv6 Router Solicitation.
Nos endereços globais (quando em auto-configuração stateless) o prefixo de rede é recebido nos pacotes "Router Advertisement" (RA) enviados pelos routers. O interface ID poderá ser construido pelo terminal de forma aleatória ou em função do seu endereço MAC de acordo com a norma EUI-64.
Para além destes pacotes, o terminal envia também mensagens MLDv2 Report.

2e) Em IPv4, o terminal irá enviar um ARP REQUEST para identificar o endereço MAC do gateway (visto o terminal de destino estar noutra rede IP). O gateway responderá com um ARP REPLY. Depois o terminal constrói o cabeçalho Ethernet e envia um pacote IP com um pacote ICMP ECHO-REQUEST. Os routers vão encaminhar o pacote até ao destino, caso não conheçam os endereços MAC dos próximos routers e do servidor irão repetir o processo de resolução ARP (REQUEST/REPLY) em cada LAN. No destino o servidor responderá com um pacote IP/ICMP ECHO-REPLY.

Em IPv6 o processo é semelhante, as únicas diferenças são: (1) o uso de pacotes ICMPv6 Neighbor-Solicitation e ICMP Neighbor-Advertisement em vez dos ARP REQUEST/REPLY e (2) os ECHO REQUEST/REPLY são pacotes ICMPv6.

3.
As tabelas de encaminhamento têm que 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 do Router2:

C redeDMZ, diretamente ligada, interface eth4
C redeR2-SWL3B, diretamente ligada, interface eth3
C redeR2-SWL3A, diretamente ligada, interface eth2
C redeR2-R1, diretamente ligada, interface eth1

R redeR1-SWL3A, [custo 1] via endIP_eth1R1, eth1
via endIP_eth1SWL3A, eth2
R redeR1-SWL3B, [custo 1] via endIP_eth1R1, eth1
via endIP_eth3SWL3B, eth3
R redeSWL3A-SWL3B, [custo 1] via endIP_eth1SWL3A, eth2
via endIP_eth3SWL3B, eth3
R redeVLAN1, [custo 1] via endIP_eth1SWL3A, eth2
via endIP_eth3SWL3B, eth3
R redeVLAN2, [custo 1] via endIP_eth1SWL3A, eth2
via endIP_eth3SWL3B, eth3
R redeVLAN3, [custo 1] via endIP_eth1SWL3A, eth2
via endIP_eth3SWL3B, eth3

(rotas por omissão obtidas por RIPv2 e RIPng)
IPv4 → R 0.0.0.0/0, via endIPv4_eth1R1, interface eth1
IPv6 → R ::/0, via endIPv6_eth1R1, interface eth1

Correção – Parte 2

1a)
As tabelas de encaminhamento tem 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 SWL3B
C redeVLAN1, diretamente ligada, interface vlan1
C redeVLAN2, diretamente ligada, interface vlan2
C redeVLAN3, diretamente ligada, interface vlan3
C redeR1-SWL3B, diretamente ligada, interface eth2
C redeR2-SWL3B, diretamente ligada, interface eth3
C redeSWL3B-SWL3A, diretamente ligada, interface eth1

O redeR1-SWL3A, [custo 20] via endIP_intVLAN1_SWL3A, interface vlan1
via endIP_intVLAN2_SWL3A, interface vlan2
via endIP_intVLAN3_SWL3A, interface vlan3
via endIP_inteth2_SWL3A, interface eth1
via endIP_inteth2_R1, interface eth2
O redeR2-SWL3A, [custo 20] via endIP_intVLAN1_SWL3A, interface vlan1
via endIP_intVLAN2_SWL3A, interface vlan2
via endIP_intVLAN3_SWL3A, interface vlan3
via endIP_inteth2_SWL3A, interface eth1
via endIP_inteth3_R2, interface eth3
O redeR1-R2, [custo 20] via endIP_eth3_R2, interface eth3
O rede DMZ, [custo 30] via endIP_eth2R1, interface eth2

(rotas por omissão obtidas por OPSF)
IPv4 → O 0.0.0.0/0, via endIPv4_eth2R1, interface eth2
IPv6 → O ::/0, via endIPv6_eth2R1, interface eth2

Nota: os interfaces LAYER 3 das VLAN (int vlan1, vlan2, vlan3) têm custo 10.

1b)
O caminho para a DMZ via SWL3B tem um custo de **40**, via R1 um custo de **30**,via R2 tem um custo de **40** e via VLANs tem um custo de **40**.
Para garantir os requisitos é preciso alterar os custos do OSPF de modo a garantir que estes caminhos têm custos sucessivamente crescentes.

Possível solução:
Aumentar o custo da interface eth0 do SWL3A para **30** (caminho =50); aumentar o custo da interface eth1 do SWL3A para **30** (caminho = 60); aumentar o custo dos interfaces VLAN do SWL3A para **60** (caminho =90).

2.

Tabela de encaminhamento IPv4 do Router A
C 210.1.1.0/27, diretamente ligada, interface eth1
C 100.0.0.0/30, diretamente ligada, interface eth0
B 193.11.11.64/26, via 100.0.0.1, interface eth0

3 a)

Terminal A	**Servidor B**
Abertura da sessão:	
TCP [SYN], SN=2000, AN=0 →	
	←TCP [SYN,ACK], SN=4000, AN=2001
TCP [ACK], SN=2001, AN=4001 →	
Troca de dados:	
	←TCP [ACK, 1500 bytes], SN=4001, AN=2001
TCP [ACK], SN=2001, AN=5501 →	
	←TCP [ACK, 1500 bytes], SN=5501, AN=2001
TCP [ACK], SN=2001, AN=7001 →	
	←TCP [ACK, 1500 bytes], SN=7001, AN=2001
TCP [ACK], SN=2001, AN=8501 →	
	←TCP [ACK, 300 bytes], SN=8501, AN=2001
TCP [ACK], SN=2001, AN=8801 →	
Finalização:	
TCP [FIN], SN=2001, AN=8801 →	
	←TCP [ACK], SN=8801, AN=2002
	←TCP [FIN], SN=8801, AN=2002
TCP [ACK], SN=2001, AN=8802 →	

3b)

No UDP não há confirmação de entrega de todos os pacotes, ou seja, não é um protocolo de transporte que garante a fiabilidade da transmissão.
É apropriado para serviços em que a entrega de todos os pacotes não seja fundamental mas sim a rapidez de entrega. Por outro lado, o UDP permite comunicações ponto-multiponto. O UDP será mais apropriado para serviços como por exemplo distribuição/difusão de vídeo, videconferência.

3c)

Devemos configurar uma ACL estendida que negue pacotes com origem nas VLAN 1 e 3 e com destino para o host Servidor B e que permita pacotes com origem na VLAN 2 e destino para o host Servidor B. Esta ACL deverá ser colocada no no interfaces dos Switches L3 A e B, no sentido de saída.

3d) Assumindo que os mecanismos de NAT/PAT já estão ativos (se não estiverem é preciso ativá-los), é preciso configurar uma associação estática de NAT/PAT que associe de forma permanente um endereço IP público ao endereço IP privado do servidor.

Nota: O NAT/PAT só começa a tradução de endereços de comunicações quando estas são iniciadas do interior da rede!

4.
Servidor DNS, v, endIPv6_DNS
Servidor mail 1, endIPv4_mail1, endIPv6_mail1 (nome: mail1.empresax.pt)
Servidor mail 2, endIPv4_mail2, endIPv6_mail2 (nome: mail2.empresax.pt)
Servidor HTTP 1, endIPv4_http1, endIPv6_http1 (nome: webmail.empresax.pt)
Servidor HTTP 2, endIPv4_http2, endIPv6_http2 (nome: webpage.empresax.pt)

DNS:

empresax.pt	**NS**	ns1.empresax.pt
empresax.pt	**MX** 10	mail1.empresa.pt
empresax.pt	**MX** 20	mail2.empresa.pt

ns1	**A**	endIPv4_DNS
ns1	**AAAA**	endIPv6_DNS
mail1	**A**	endIPv4_mail1
mail1	**AAAA**	endIPv6_mail1
mail2	**A**	endIPv4_mail2
mail2	**AAAA**	endIPv6_mail2

webmail	**A**	endIPv4_http1
webmail	**AAAA**	endIPv6_http1
webpage	**A**	endIPv4_http2
webpage	**AAAA**	endIPv6_http2

5.

É preferível o IMAP porque permite (i) criar e gerir um sistema de diretórios de mensagens no servidor; (ii) fazer operações de procura no sistema de directórios – útil para utilizadores que usem o serviço de múltiplos terminais; (iii) solicitar o envio de partes das mensagens de correio – útil quando o terminal está ligado à rede através de ligações de baixo débito.