

Correção

1a)

O switch/bridge raiz é o Switch2 porque é o switch com o menor ID (menor MAC address).

	Custo para a raiz (RPC)	Porta raiz	Portas bloqueadas	Justificações
Switch 1	5	1	2	A porta 1 é raiz. A porta 2 fornece um RPC igual ao da porta 1 do switch 5 (RPC=5) mas o ID do switch 5 é menor, logo a porta 2 do switch 1 está bloqueada.
Switch 2	-	-	-	É o switch raiz, todas as portas são designadas.
Switch 3	20	1	2	A porta 1 é raiz, já que fornece uma ligação direta para a raiz, com custo de 20. A porta 2 está bloqueada já que o RPC pelo switch 4 é menor (10).
Switch 4	10	3	2	A porta 3 é raiz, já que fornece uma ligação direta para a raiz, com custo de 10. A porta 2 está bloqueada já que o RPC pelo switch 5 é menor (5). A porta 1 é designada.
Switch 5	5	3	-	Porta 3 é raiz, portas 1 e 2 são designadas (fornecem melhor caminho para a raiz em relação aos SW1 e SW4).
SWL3 A	5	1	-	A porta 1 é raiz, já que fornece uma ligação direta para a raiz, com custo de 5. A porta 2 é designada já que o RPC pelo SWL3 B é igual (5) mas o ID do SWL3 B é maior.
SWL3 B	5	1	2	A porta 1 é raiz, já que fornece uma ligação direta para a raiz, com custo de 5. A porta 2 está bloqueada já que o RPC pelo SWL3 A é igual (5) mas o ID do SWL3 A é menor.

1b) Se o switch 5 avariar deixará de enviar BPDUs para as LANs em que é designado. Quando o contador **age** igualar **max age**, os switches 1 e 4 assumem que são designados nas LANs ligadas ao switch 5 e as respetivas portas 2 passam a designadas.

1c) Claro que sim. Passaria a haver loops lógicos e qualquer pacote que fosse enviado para o endereço de broadcast ethernet (FF:FF:FF:FF:FF:FF) passaria a circular indefinidamente na rede de switches. A rede de switches ficaria inoperacional.

2a)

Endereçamento público:

A VLAN2 precisa de 21 endereços IPv4 públicos, logo a sub-rede deverá ter um tamanho de 32 (21+2 routers+ID+Broadcast=25 → 32); máscara /27.

A rede do DMZ precisa de 15 endereços IPv4 públicos, logo a sub-rede deverá ter um tamanho de 32 (15+1 routers+ID+Broadcast=18 → 32); máscara /27.

O NAT precisa de 12 endereços IPv4 públicos, logo a sub-rede deverá ter um tamanho de 16 (12+ID+Broadcast=14 → 16); máscara /28.

O Datacenter precisa de 10 endereços IPv4 públicos, logo a sub-rede deverá ter um tamanho de 16 (10+Router + ID+Broadcast=13 → 16); máscara /28.

Começando da rede maior e a partir de 193.5.5.0/25:

VLAN 2	193.5.5.0/27 (+32 endereços)
DMZ	193.5.5.32/27 (+32 endereços)
Datacenter	193.5.5.64/28 (+16 endereços)
NAT	193.5.5.80/28 (+16 endereços)
Livre	193.5.5.96/27

Endereçamento privado:

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 192.168.0.0/16, 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.

Possível solução:

VLAN1	192.168.1.0/24
VLAN2	192.168.2.0/24
Datacenter	192.168.3.0/24
DMZ	192.168.4.0/24
Rede R1-R3	192.168.5.0/30
Rede R1-SWL3A	192.168.5.4/30
Rede R1-R2	192.168.5.8/30
Rede R3-SWL3A	192.168.5.10/30
Rede R3-SWL3B	192.168.5.12/30
Rede R3-R2	192.168.5.14/30
Rede R2-SWL3B	192.168.5.16/30

2b)

A rede IPv6 disponível é 2200:1:1:10::/56 logo pode-se definir qualquer endereço que comece por 2200:1:1:10XX: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 2200:1:1:10XY::/64 com X e Y a variarem de 0 a F.

Possível solução:

VLAN1	2200:1:1:1001::/64
VLAN2	2200:1:1:1002::/64
Datacenter	2200:1:1:1003::/64
DMZ	2200:1:1:1004::/64
Rede R1-R3	2200:1:1:1005::/64

Rede R1-SWL3A	2200:1:1:1006::/64
Rede R1-R2	2200:1:1:1007::/64
Rede R3-SWL3A	2200:1:1:1008::/64
Rede R3-SWL3B	2200:1:1:1009::/64
Rede R3-R2	2200:1:1:100A::/64
Rede R2-SWL3B	2200:1:1:100B::/64

2c)

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 (endereço IP da VLAN 1 do SWL3B) responderá com um ARP REPLY. Depois o terminal constrói o cabeçalho Ethernet e envia um pacote IP com um pacote ICMP ECHO-REQUEST para o SWL3B. 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 que fará o percurso de custo mínimo em direção à VLAN 1.

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.

2d)

Em todos os switches L2 será necessário configurar portas de acesso pertencentes à VLAN 3. As portas trunk (dot1q) já servirão para encaminhar pacotes da VLAN 3. Nos switches L3 é necessário configurar a VLAN 3 (interface virtual) e adicionar a respetiva rede IPv4 e IPv6 aos protocolos de encaminhamento.

3.

a)

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 Router 3:

C	redeR3-R1, diretamente ligada, interface eth0
C	redeR3-SWL3A, diretamente ligada, interface eth1
C	redeR3-SWL3B, diretamente ligada, interface eth3
C	redeR3-R2, diretamente ligada, interface eth2
R	redeR1-SWL3A, [custo 1] via endIP_eth3R1, eth0 via endIP_eth1SWL3A, eth1
R	redeR2-SWL3B, [custo 1] via endIP_eth2R2, eth2 via endIP_eth1SWL3B, eth3
R	redeR1-R2, [custo 1] via endIP_eth3R1, eth0 via endIP_eth2R2, eth2
R	redeDMZ, [custo 1] via endIP_eth3R1, eth0
R	redeDatacenter, [custo 1] via endIP_eth2R2, eth2
R	redeVLAN1, [custo 1] via endIP_eth1SWL3A, eth1 via endIP_eth1SWL3B, eth3
R	redeVLAN2, [custo 1] via endIP_eth1SWL3A, eth1 via endIP_eth1SWL3B, eth3

(rota por omissão obtida por RIPv2)

IPv4 → R 0.0.0.0/0, via endIPv4_eth3R1, interface eth0

3b)

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!).

C	redeR3-R1, diretamente ligada, interface eth0
C	redeR3-SWL3A, diretamente ligada, interface eth1
C	redeR3-SWL3B, diretamente ligada, interface eth3
C	redeR3-R2, diretamente ligada, interface eth2
<hr/>	
O	redeR1-SWL3A, [custo 12] via endIPv6_eth1SWL3B, eth3
O	redeR2-SWL3B, [custo 11] via endIPv6_eth1SWL3B, eth3
O	redeR1-R2, [custo 15] via endIPv6_eth3R1, eth0
O	redeDMZ, [custo 15] via endIPv6_eth3R1, eth0
O	redeDatacenter, [custo 21] via endIPv6_eth1SWL3B, eth3
O	redeVLAN1, [custo 2] via endIPv6_eth1SWL3B, eth3
O	redeVLAN2, [custo 2] via endIPv6_eth1SWL3B, eth3
(rota por omissão obtida por OPSF)	
O	::/0, via endIPv6_eth3R1, interface eth0

Nota: os interfaces LAYER 3 das VLAN (int vlan1, vlan2) têm custo 1.

3c)

O caminho desde o SWL3B até ao Datacenter tem os seguintes custos: **20** via eth3 do R2, **31** via VLAN 1 ou VLAN 2 do SWL3A; **35** via eth3 do R3.

Para garantir os requisitos é preciso alterar os custos do OSPF de modo a garantir que estes caminhos têm custos sucessivamente crescentes.

Possível solução:

Reduzir o custo da interface eth1 do SWL3B para **1** (caminho = 26 através do R3); aumentar o custo da interface eth1 do SWL3A para **30** (caminho = 60); aumentar o custo dos interfaces VLAN do SWL3A para **60** (caminho =90).

4a)

Deverá configurar os atributos **Local Preference** nos Routers A e B, com um valor maior no Router A.

4b)

O Next-Hop tem o valor 100.0.0.1.

5)

Devemos configurar uma ACL estendida que negue pacotes com origem na VLAN 2 e com destino para o host Servidor B e que permita todos os restantes pacotes. Esta ACL deverá ser colocada nos interfaces eth0 e eth1 dos Switches L3 A e B, no sentido de saída.

6)

O servidor proxy actua como um elemento intermédio entre o cliente e o servidor, ou seja, o cliente interage com o Servidor Proxy como se ele fosse o servidor Web. O Servidor Proxy interage com os servidores Web em nome dos clientes. O servidor Proxy armazena todos os ficheiros pedidos pelos clientes (até ao limite da sua capacidade de armazenamento).

Os servidores proxy nas empresas: diminuem os tempos de interação, reduzem o tráfego para a rede pública. Os servidores proxy nas redes dos Internet Service Providers (ISPs): permitem uma infraestrutura de distribuição automática dos conteúdos Web mais solicitados por elementos de rede que estão topologicamente perto dos clientes.