Dicas de Correção do Exame de Redes e Serviços
14 de Janeiro de 2020

1a)

O switch/bridge raiz é o Switch 5, porque é o switch com o menor ID (prioridade 6999h e MAC Address AA:44:44:44:44:44).

	Custo para a raiz (RPC)	Porta raiz	Portas designadas	Portas bloqueadas	Justificações
Switch 1	5	2	1,4	3	Este switch fornece o percurso de custo mínimo para a raiz (5) para a LAN entre o SWL3A e o SW1.
Switch 2	5	2	3	1,4	Este switch fornece o percurso de custo mínimo para a raiz (5) para as LANs entre o SW1 e o SW2 e entre o SW2 e o SW3.
Switch 3	10	4	--	1,2,3	
Switch 4	5	2	1,3,4	--	Fornece o percurso de custo mínimo em todas as LANs a que está ligado..
Switch 5	0	--	1,2,3,4,5,6	--	Switch raiz.
SWL3 A	5	F1/1	F1/3	F1/0,f1/2	Não tem portas designadas porque nunca fornece o percurso de custo mínimo.
SWL3 B	5	F1/1	F1/0,f1/2	--	Este switch fornece o percurso de custo mínimo para a raiz (5) para as LANs entre o SWL3A e o SWL3B e entre o SW3 e o SWL3B.

1b)

Permite configurar spanning trees diferentes por cada VLAN, cada uma com a sua raiz e as suas portas designadas. Em função do número de utilizadores em cada LAN e da carga de tráfego previsível em cada troço da rede, é possível ter diferentes redes lógicas sobre a mesma rede física.

2a)
PÚBLICO:

A VLAN 4 precisa de 50 IPv4 públicos, logo a sub-rede deverá ter um tamanho de 64 (50+2 routers+ID+Broadast=54 → 64); máscara /26.

A VLAN 1 precisa de 22 IPv4 públicos, logo a sub-rede deverá ter um tamanho de 32 (22+2 routers+ID+Broadast=26 → 32); máscara /27.

A VLAN 2 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 rede do DC precisa de 8 IPv4 públicos, logo a sub-rede deverá ter um tamanho de 16 (8+4 routers+ID+Broadast=14 → 16); máscara /28.

A rede do DMZ precisa de 6 IPv4 públicos, logo a sub-rede deverá ter um tamanho de 8 (6+2 routers+ID+Broadast=10 → 16); máscara /28.

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

Fazendo subnetting da rede 191.1.1.0/24:

191.1.1.xx/26, em que xx pode ser 00, 01, 10 ou 11, obtemos as seguintes subredes:

VLAN4	**191.1.1.0/26**
	191.1.1.128/26
	191.1.1.64/26
	191.1.1.192/26

Fazendo subnetting da rede 191.1.1.128/26:

191.1.1.10x/27, em que x pode ser 0 ou 1, obtemos as seguintes subredes:

VLAN1	**191.1.1.128/27**
VLAN2	**191.1.1.160/27**

Fazendo subnetting da rede 191.1.1.64/26:

191.1.1.01xx/28, em que x pode ser 00, 01, 10 ou 11, obtemos as seguintes subredes:

DC	**191.1.1.64/28**
DMZ	**191.1.1.80/28**
	191.1.1.96/28
Livre	**191.1.1.112/28**

Fazendo subnetting da rede 191.1.1.96/28:

193.3.3.0110x/28, em que x pode ser 0 ou 1, obtemos as seguintes subredes:

NAPT	**191.1.1.112/29**
Livre	**191.1.1.120/29**

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
VLAN4	192.168.4.0/24
Datacenter	192.168.5.0/24
DMZ	192.168.6.0/24
Rede SWL3A-R3	192.168.7.0/24
Rede R2-R3	192.168.8.0/24
Old building	192.168.9.0/24
Site B	192.168.10.0/24

A rede IPv6 disponível é 2001:1:1::/60 logo pode-se definir qualquer endereço que comece por 2001:1:1:000X::/64 (a máscara fixa os primeiros 60 bits do endereço). Pode-se/deve-se assumir redes com máscara /64.

VLAN1	2001:1:1:0::/64
VLAN2	2001:1:1:1::/64
VLAN3	2001:1:1:2::/64
VLAN4	2001:1:1:3::/64
Datacenter	2001:1:1:4::/64
DMZ	2001:1:1:5::/64
Rede SWL3A-R3	2001:1:1:6::/64
Rede R2-R3	2001:1:1:7::/64
Old building	2001:1:1:8::/64
Site B	2001:1:1:9::/64

2b)

Neste caso, será necessário despoletar o processo de descoberta do endereço MAC do default gateway (endereço VLAN 3 do SWL3B).
IPv4: O PC A irá enviar um ARP Request pela rede de switches (em flooding) com o objetivo de descobrir o MAC Address do Default Gateway. O SWL3 B responderá com um ARP Reply pela rede de switches até ao PC A. O PC A envia um ICMP Echo Request em direção ao SWL3 B (PC A → SW4 → SW5 → SWL3B). Este por sua vez irá enviar um ARP Request pela rede de switches (na VLAN 3) com o objetivo de descobrir o MAC Address do PC B. Este responderá com um ARP Reply pelo percurso PC B → SWL3 A → SW5 → SWL3 B. O ICMP Echo Request será então enviado para o PC B pelo percurso inverso. O Echo Reply fará o percurso PC B → SWL3 A → SW5 → SW4 → PC A. Note-se que as tabelas de MAC Address dos swicthes irão sendo construídas durante este processo.
IPv6: O terminal irá enviar um pacote ICMPv6 Neighbor-Solicitation para o endereço multicast Solicited-Node, tendo como endereço origem o seu endereço IPv6 Global, com o objetivo de descobrir o endereço físico do Default Gateway (endereço da interface VLAN 3 do SWL3B). 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 VLAN 3 do SWL3B.
Este swicth irá repetir o mesmo processo para descobrir o MAC do PC B, enviando-lhe depois o pacote ICMPv6 ECHO REPLY para o seu endereço IPv6 Global.

O PCB irá responder com o ICMPv6 ECHO REPLY, via redes de switches, PC B → SWL3 A → SW5 → SW4 → PC A.

3. a)
A rota estática tem que ser redistribuída no router 3 para o processo RIP:
router rip
redistribute static metric <inteiro>

Dessa forma, irá ser propagada por RIP ao Router 1 e ao SWL3 A e daí será feita a redistribuição do RIP n OSPF para toda a rede por OSPF.
Obviamente que se supõe que o router de saída do Site B tem uma rota estática ou rota por omissão a apontar para o Router 3.

b) 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!).

Vamos assumir que na redistribuição OSPF → RIP é usada uma métrica de 2 para todas as redes.

Tabela de encaminhamento IPv4 do Router 3
C rede OldBuilding, diretamente ligada, interface eth3
C rede R3_SiteB, diretamente ligada, interface eth4
C redeR3-R2, diretamente ligada, interface eth1
C redeR3-SWL3A, diretamente ligada, interface eth2

S rede_SiteB[1/0], via 11.11.11.2, interface eth4

R redeDatacenter [110/3], via eth3R2, interface eth1
via eth2SWL3A, interface eth2
R redeDMZ [110/3], via eth3R2, interface eth1
via eth2SWL3A, interface eth2
R rede_VLAN1, [110/3] , via eth3R2, interface eth1
via eth2SWL3A, interface eth2
R rede_VLAN2, [110/3] , via eth3R2, interface eth1
via eth2SWL3A, interface eth2
R rede_VLAN3, [110/3] , via eth3R2, interface eth1
via eth2SWL3A, interface eth2
R rede_VLAN4, [110/3] , via eth3R2, interface eth1
via eth2SWL3A, interface eth2

(rota por omissão obtida por RIP)
R 0.0.0.0/0, [110/3] , via eth3R2, interface eth1
via eth2SWL3A, interface eth2

c)
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!).

Vamos assumir que na redistribuição RIP → OSPF é usada uma métrica de 1 para todas as redes.

Tabela de encaminhamento IPv6 do SWL3B
C rede DC, diretamente ligada, interface eth1
C rede VLAN1, diretamente ligada, interface VLAN1
C rede VLAN2, diretamente ligada, interface VLAN2
C rede VLAN3, diretamente ligada, interface VLAN3

C rede VLAN4, diretamente ligada, interface VLAN4

O rede DMZ[110/15], via eth2R1, interface eth1
via eth2R2, interface eth1
via VLAN1SWL3A, interface VLAN1
via VLAN2SWL3A, interface VLAN2
via VLAN3SWL3A, interface VLAN3
via VLAN4SWL3A, interface VLAN4
OE2 rede SWL3A-R3[110/6], via VLAN1SWL3A, interface VLAN1
via VLAN2SWL3A, interface VLAN2
via VLAN3SWL3A, interface VLAN3
via VLAN4SWL3A, interface VLAN4
OE2 rede R2-R3[110/11], via eth2R2, interface eth1
via VLAN1SWL3A, interface VLAN1
via VLAN2SWL3A, interface VLAN2
via VLAN3SWL3A, interface VLAN3
via VLAN4SWL3A, interface VLAN4
OE2 rede OldBuilding[110/6], via VLAN1SWL3A, interface VLAN1
via VLAN2SWL3A, interface VLAN2
via VLAN3SWL3A, interface VLAN3
via VLAN4SWL3A, interface VLAN4
OE2 rede siteB[110/6], via VLAN1SWL3A, interface VLAN1
via VLAN2SWL3A, interface VLAN2
via VLAN3SWL3A, interface VLAN3
via VLAN4SWL3A, interface VLAN4

(rota por omissão obtida por OSPF, assumindo que ela é anunciada com métrica de 1)
OE2 0.0.0.0/0, [110/11], via eth2R2, interface eth1
via eth2R1, interface eth1
via VLAN1SWL3A, interface VLAN1
via VLAN2SWL3A, interface VLAN2
via VLAN3SWL3A, interface VLAN3
via VLAN4SWL3A, interface VLAN4
---

d)
Há várias soluções:

- A rota por omissão anunciada pelo Router 2 deve ser do tipo E2 e ter um métrica inferior à rota por omissão anunciada pelo router 1:
  default-information originate always metric <inteiro>

- Caso as rotas anunciadas sejam do tipo E1, temos que garantir que a soma do custo para o Router 2 com a métrica anunciada na rota seja inferior à soma do custo para o Router 1com a métrica anunciada na rota.

- Pode-se ainda criar uma rota estática por omissão nos SWL3A e SWL3B.

4.

C 210.1.1.32/27, directly connected, eth1
C 210.1.1.64/27, directly connected, eth2
C 100.0.0.0/30, directly connected, eth0
B 191.1.1.0/25 [20/0], via 100.0.0.6, eth0

5)

Configurar um ou vários (por questões de redundância) servidores de DHCP, desde que as gamas de endereços configuradas nos vários servidores sejam disjuntas. Neste caso, configuraria no SWL3 A ou B (para servir os clientes das VLANs) e outro no Datacenter. É necessário ativar o DHCP Relay Agent para que as mensagens DHCP passem pelos routers.

6)

i)
Colocar nas interfaces eth0 dos routers 1 e 2 (sentido de entrada) uma ACL extended que negue o protocolo icmp para todos os endereços das redes IPv4 191.1.1.0/24 e IPv6 2001:1:1::/60:
access-list 101 deny icmp any 191.1.1.0 0.0.0.255
access-list 101 deny icmpv6 any 2001:1:1::/60
access-list 101 permit ip any any
access-list 101 permit ipv6 any any

ii)
Colocar na interface VLAN 3 dos SWL3 A e B (sentido de entrada) uma ACL extended que negue o tráfego destinado ao servidor HTTP localizado na DMZ (tanto em IPv4 como em IPv6):
access-list 102 deny ip IPv4Privado_VLAN3 IPServidor eq 80
access-list 102 deny ipv6 IPv6_VLAN3 IPv6Servidor eq 80
access-list 102 permit ip any any
access-list 102 permit ipv6 any any

7)

Para comunicação com o exterior: NAT/PAT dinâmico nos routers 1 e 2 (não sabemos por onde será feita a saída da rede).Configura-se uma pool de endereços de acordo com o subnetting feito na questão 2ª), uma ACL que define os endereços que serão traduzidos e definem-se quais são as portas inside e outside.

Para comunicação do exterior para o interior da empresa: deveria configurar uma entrada NAT/PAT estática que associasse um IP público da rede reservada para o NAT ao IP privado do servidor de FTP. Isso deverá ser feito nos routers de entrada da rede (R1 e/ou R2).

8)
PIM, dense mode:
A maioria das redes têm estações que pretendem usar encaminhamento multicast.
Implementa uma estratégia "RPF com pruning"; exige que todos os routers tenham o protocolo activo; os routers reencaminham por omissão para todos os vizinhos que não tenham enviado mensagens de prune; usam as mensagens de prune para sinalizar os vizinhos que não devem reencaminhar os pacotes para eles
PIM, sparse mode:
As estações que pretendem usar encaminhamento multicast concentram-se num número reduzido de redes.
Cada router anuncia explicitamente (com mensagens Join) que quer suportar determinadas sessões multicast.