Dicas de Correção do Exame de Redes e Serviços
10 de fevereiro de 2022

1a)

O switch/bridge raiz é o SWL3A, porque é o switch com o menor ID (prioridade 6999h, igual à dos SW2 e SW5 mas com menor MAC address).

	Custo para a raiz (RPC)	Porta raiz	Portas designadas	Portas bloqueadas	Justificações
Switch 1	5	2	3,4	1	A porta 1 está bloqueada, porque embora proporcione um custo de 5 para a raiz, tal como a porta f1/1 do SWL3B, o ID deste switch é menor.
Switch 2	10	2	3,4	1	
Switch 3	15	1	--	2,3,4	A porta 4 está bloqueada, porque embora proporcione um custo de 15 para a raiz, tal como a porta 1 do SW5, o ID deste switch é menor.
Switch 4	10	2	3,4	1	
Switch 5	15	2	1	--	
SWL3 A	0	--	f1/0,f1/1,f1/2	--	Switch raíz. Todas as portas são designadas.
SWL3 B	5	f1/2	f1/1	--	

b)
Em termos da localização da raíz, a ST já está otimizada. No entanto, poderiamos configurar o protocolo Rapid ST, que é mais rápido na resposta a alterações na tolopogia.

2a)
PÚBLICO:

A VLAN1 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 VLAN21 precisa de 12 IPv4 públicos, logo a sub-rede deverá ter um tamanho de 16 (12+1 router+ID+Broadast=15 → 16); máscara /28.

A VLAN23 precisa de 10 IPv4 públicos, logo a sub-rede deverá ter um tamanho de 16 (10+1 router+ID+Broadast=13 → 16); máscara /28.

A rede do DC precisa de 8 IPv4 públicos, logo a sub-rede deverá ter um tamanho de 16 (8+1 router+ID+Broadast=11 → 16); máscara /28.

A rede do DMZ precisa de 3 IPv4 públicos, logo a sub-rede deverá ter um tamanho de 8 (3+1 router+ID+Broadast=6 → 8); máscara /29.

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 193.1.1.0/25:

193.1.1.0xx/27, em que x pode ser 00, 01, 10 ou 11, obtemos as seguintes subredes:

VLAN1	**193.1.1.0/27**
	193.1.1.32/27
	193.1.1.64/27
	193.1.1.96/27

Fazendo subnetting da rede seguinte que está livre (193.1.1.32/27):

193.1.1.001x/28, em que x pode ser 0 ou 1, obtemos as seguintes subredes:

VLAN21	**193.1.1.32/28**
VLAN23	**193.1.1.48/28**

A rede 193.1.1.32/27 já está utilizada. Fazendo subnetting da rede seguinte que está livre (193.1.1.64/27):

193.1.1.010x/28, em que x pode ser 0 ou 1, obtemos as seguintes subredes:

DC	**193.1.1.64/28**
	193.1.1.80/28

Fazendo subnetting da rede 193.1.1.80/28):

193.1.1.0101x/28, em que x pode ser 0 ou 1, obtemos as seguintes subredes:

DMZ	**193.1.1.80/29**
NAT	**193.1.1.88/29**

A subrede 193.1.1.96/27 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
VLAN21	192.168.2.0/24
VLAN22	192.168.3.0/24
VLAN23	192.168.4.0/24
Datacenter	192.168.5.0/24
DMZ	192.168.6.0/24
Rede SWL3C-SWL3B	192.168.7.0/24

Rede SWL3C-SWL3A	192.168.8.0/24
Rede R2-SWL3C	192.168.9.0/24
Rede R2-R1	192.168.10.0/24

A rede IPv6 disponível é 2100:2100::/60 logo pode-se definir qualquer endereço que comece por 2100:2100:0000:000X::/64 (a máscara fixa os primeiros 60 bits do endereço). Pode-se/deve-se assumir redes com máscara /64.

VLAN1	2100:2100:0:0::/64
VLAN21	2100:2100:0:1::/64
VLAN22	2100:2100:0:2::/64
VLAN23	2100:2100:0:3::/64
Datacenter	2100:2100:0:4::/64
DMZ	2100:2100:0:5::/64
Rede SWL3C-SWL3B	2100:2100:0:6::/64
Rede SWL3C-SWL3A	2100:2100:0:7::/64
Rede R2-SWL3C	2100:2100:0:8::/64
Rede R2-R1	2100:2100:0:9::/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 SW5 → SW4 → SW1 → SWL3A) .
Este switch irá repetir o mesmo processo para descobrir o MAC do interface eth2 do Router 1, enviando-lhe o pacote ICMPv6 ECHO REPLY para o seu endereço IPv6 Global. O Router 1, por sua vez, fará o mesmo para descobrir o MAC address do PCB. O PCB irá responder com o ICMPv6 ECHO REPLY, via R1→SWL3A→ SW1→SW4→SW5 até ao PCB.

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 (percurso SW5 → SW4 → SW1 → SWL3A) .
Este switch irá repetir o mesmo processo para descobrir o MAC do interface eth2 do Router 1, enviando-lhe o pacote ARP Request e recebendo um ARP REPLY. Depois envia o ICMP ECHO REQUEST. O Router 1 irá fazer o mesmo procedimento para descobrir o MAC address do PCB, enviando-lhe o ICMP Echo Request. O PC B irá responder com o ICMP ECHO REPLY, via R1, SWL3A e redes de switches, SW1, SW1 e SW5 até ao PCA.

2c)
Colocaria um servidor de DHCP/DHCPv6 na VLAN 1, por exemplo. Neste caso, só teria que configurar a pool de endereços e os diferentes parâmetros a atribuir, tais como default gateway, servidor de DNS, etc. Caso optasse por colocar o servidor no DC, por exemplo, para além da configuração do próprio servidor, teria também que ativar no interfaces VLAN 1 dos SWL3A e B, nos interfaces do SWL3C e do Router 2 o Realy Agent para que estes routers reencaminhassem pos pacotes BootP para o Datacenter.

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	redeSWL3A-Router2, diretamente ligada, interface eth2	
C	redeSWL3A-SWL3C, diretamente ligada, interface eth1	
R	redeSWL3C-SWL3B, [120/custo 1]	via endIP_VLAN1_SWL3B, interface vlan1 via endIP_eth2_SWL3C, interface eth1
R	redeVLAN21, [120/custo 1]	via endIP_eth2_SWL3C, interface eth1
R	redeVLAN22, [120/custo 1]	via endIP_eth2_SWL3C, interface eth1
R	redeVLAN23, [120/custo 1]	via endIP_eth2_SWL3C, interface eth1
R	redeSWL3C-R1, [120/custo 1]	via endIP_eth2_SWL3C, interface eth1
R	redeSWL3C-R2, [120/custo 1]	via endIP_eth2_SWL3C, interface eth1 via endIP_eth3_R2, interface eth2
R	redeR2-R1, [120/custo 1]	via endIP_eth3_R2, interface eth2
R	redeDC, [120/custo 1]	via endIP_eth3_R2, interface eth2
R	redeDMZ, [120/custo 2]	via endIP_eth3_R2, interface eth2 via endIP_eth2_SWL3C, interface eth1

(rota por omissão obtida por OSPF)

R 0.0.0.0/0, [120/custo 2]	via endIP_eth3_R2, interface eth2 via endIP_eth2_SWL3C, interface eth1

b)
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:
Aumentar o custo da interface eth2 do SWL3A para 15 e da interface eth3 do SWL3C para 15. Assim o custo do caminho SWL3A → SWL3C → Router1 fica igual a 10. O custo do caminho SWL3B → SWL3C → Router1 fica igual a 10. Todos os caminhos que passam pelo Router 2 terão custo superior.

4. a)
Asumindo que se sabe os números dos Sistemas Autónomos do Irão (base de dados pública) define-se uma regra que estabelece que quando se recebe um UPDATE para uma rede da Austrália com um atributo **AS_PATH** que contenha os números de Sistemas Autónomos do Irão se baixe a preferência local (**LOCAL PREFERENCE**) dessa(s) rota(sd).

b)
Todos os anúncios de rotas recebidos do vizinho sem limitações de tráfego deverão ter uma preferência local maior (**LOCAL PREFERENCE maior**). O atributo LOCAL PREFERENCE será colocado em todos os an+uncios enviados para os vizinhos BGP internos.

5)
Uma associação de segurança (SA) representa um contrato de política de segurança entre dois peers ou hosts e descreve como é que os peers irão usar os serviços IPSec para proteger o tráfego da rede. A SA contém os seguintes parâmetros:

- algoritmo de autenticação/encriptação, comprimento da chave e outros parâmetros de encriptação (e.g. tempo de vida da chave, ...)
- chaves para autenticação e encriptação
- especificação do tráfego ao qual o SA será aplicado
- protocolos de IPSec AH ou de ESP e especificação do modo túnel ou transporte.

6)
Colocaria na interface eth0 do SWL3C uma **ACL estendida** que impedisse todo o tráfego FTP proveniente da VLAN 21 e destinado ao servidor de FTP localizado na DMZ:

access-list 101 deny ip IPv4_VLAN21 IPv4_servidorFTP eq 21
access-list 101 deny ip IPv4_VLAN21 IPv4_servidorFTP eq 20
access-list 101 deny ip IPv6_VLAN21 IPv6_servidorFTP eq 21
access-list 101 deny ip IPv6_VLAN21 IPv6_servidorFTP eq 20
acces-list 101 permit any any

Finalmente, aplicaria no interface **eth0**, no sentido **in**