

Dicas de Correção do Exame de Recurso de Redes e Serviços
31 de Janeiro de 2019

1a)

O switch/bridge raiz é o Switch 2, porque é o switch com o menor ID (prioridade 6000h e MAC Address CC:24:24:24:24:24).

	Custo para a raiz (RPC)	Porta raiz	Portas designadas	Portas bloqueadas	Justificações
Switch 1	10	5	1,2,3,4	--	Este switch fornece o percurso de custo mínimo para a raiz em todas as LANs a que está ligado.
Switch 2	0	--	1,2,3	--	Switch raiz.
Switch 3	20	4	1,2	3	A porta 3 está bloqueada porque o switch 1 fornece um custo menor para a raiz, comparativamente com o switch 3. A porta 2 é designada porque o switch 3 proporciona o mesmo custo para a raiz do que o Switch 5 mas tem um ID menor.
Switch 4	15	2	1,4	3	A porta 3 está bloqueada porque a porta raiz é a porta 2.
Switch 5	20	4	3	1,2	As portas 1 e 2 estão bloqueadas porque os switches 1 e 3 (respetivamente) fornecem percursos de custo mínimo para a raiz.
SWL3 A	15	1	2,3	--	
SWL3 B	25	1	--	2,3	O percurso através do switch 3 tem o menor custo para a raiz. As portas 2 e 3 estão bloqueadas porque os switches 1 e SWL3A (respetivamente) fornecem percursos de custo mínimo para a raiz.

1b)

Note-se que todas as comunicações passam pelos PCA → SW1 → SW2 → SW4 → PCB.
Tabela de encaminhamento Layer 2 (forwarding table) do SW4.

Endereço MAC	Porta (do próprio switch)
MAC_terminalA	2
MAC_terminalB	4
SWL3B	1
Switch 1	2 (MAC aprendido com os pacotes da Spanning-tree)
Switch 2	3 (MAC aprendido com os pacotes da Spanning-tree)
Switch 3	1 (MAC aprendido com os pacotes da Spanning-tree)

2a)

PÚBLICO:

A VLAN 2 precisa de 35 IPv4 públicos, logo a sub-rede deverá ter um tamanho de 64 ($31+2 \text{ routers} + \text{ID} + \text{Broadcast} = 35 \rightarrow 64$); máscara /26.

A VLAN 3 precisa de 18 IPv4 públicos, logo a sub-rede deverá ter um tamanho de 32 ($14+2 \text{ routers} + \text{ID} + \text{Broadcast} = 18 \rightarrow 32$); máscara /27.

A rede do DC precisa de 12 IPv4 públicos, logo a sub-rede deverá ter um tamanho de 16 ($6+4 \text{ routers} + \text{ID} + \text{Broadcast} = 12 \rightarrow 16$); máscara /28.

A rede do DMZ precisa de 7 IPv4 públicos, logo a sub-rede deverá ter um tamanho de 8 ($3+2 \text{ routers} + \text{ID} + \text{Broadcast} = 7 \rightarrow 8$); máscara /29.

O NAT precisa de 7 IPv4 públicos, logo a sub-rede deverá ter um tamanho de 8 ($5 + \text{ID} + \text{Broadcast} = 7 \rightarrow 8$); máscara /29.

Fazendo subnetting da rede 193.3.3.0/25:

195.5.5.0x/26, em que x pode ser 0 ou 1, obtemos as seguintes subredes:

VLAN2	195.5.5.0/26
	195.5.5.64/26

Fazendo subnetting da rede 195.5.5.64/26:

195.5.5.01x/27, em que x pode ser 0 ou 1, obtemos as seguintes subredes:

VLAN3	195.5.5.64/27
	195.5.5.96/27

Fazendo subnetting da rede 195.5.5.96/27:

193.3.3.011x/28, em que x pode ser 0 ou 1, obtemos as seguintes subredes:

DC	195.5.5.96/28
	195.5.5.112/28

Fazendo subnetting da rede 195.5.5.112/28:

193.3.3.0111x/28, em que x pode ser 0 ou 1, obtemos as seguintes subredes:

DMZ	195.5.5.112/29
NAPT	195.5.5.120/29

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
Datacenter	192.168.4.0/24
DMZ	192.168.5.0/24
Rede SWL3A-R2	192.168.6.0/24
Rede SWL3B-R1	192.168.7.0/24

A rede IPv6 disponível é 2000:2000:2000::/56 logo pode-se definir qualquer endereço que comece por 2000:2000:2000:00XX::/64 (a máscara fixa os primeiros 56 bits do endereço). Pode-se/deve-se assumir redes com máscara /64.

VLAN1	2000:2000:2000:0000::/64
VLAN2	2000:2000:2000:0001::/64
VLAN3	2000:2000:2000:0002::/64
Datacenter	2000:2000:2000:0003::/64
DMZ	2000:2000:2000:0004::/64
Rede SWL3A-R2	2000:2000:2000:0005::/64
Rede SWL3B-R1	2000:2000:2000:0006::/64

2b)

Os pacotes que são enviados para um endereço anycast serão capturados pelo dispositivo mais próximo. Por essa razão, hoje em dia estes endereços são usados pelo serviço DNS proporcionado pelos servidores raiz.

O endereços anycast são sintacticamente indistinguíveis dos endereços unicast, porque são alocados a partir do mesmo espaço de endereçamento unicast.

2c)

Neste caso, será necessário despoletar o processo de descoberta do endereço MAC do default gateway (endereço VLAN 1 do SWL3B). 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 VLAN 1 do SWL3B.

Este swithc irá repetir o mesmo processo para descobrir o MAC do PCB, 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, SW4, SW1 e SW2 até ao PCA.

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 IPv4 do SWL3B

C	redeVLAN1, diretamente ligada, interface vlan1	
C	redeVLAN2, diretamente ligada, interface vlan2	
C	redeVLAN3, diretamente ligada, interface vlan2	
C	redeDatacenter, diretamente ligada, interface eth1	
C	redeSWL3B-R1, diretamente ligada, interface eth0	
O	redeSWL3A-R2, [110/custo 10]	via endIP_VLAN1_SWL3A, interface vlan1 via endIP_VLAN2_SWL3A, interface vlan2 via endIP_VLAN3_SWL3A, interface vlan3
O	redeDMZ, [110/custo 15]	via endIP_eth1_Router1, eth1 via endIP_eth2_Router2, eth1 via endIP_eth3_Router1, eth0 via endIP_VLAN1_SWL3A, interface vlan1 via endIP_VLAN2_SWL3A, interface vlan2 via endIP_VLAN3_SWL3A, interface vlan3

(rota por omissão obtida por RIP)

R 0.0.0.0/0, [120/custo 1]	via endIP_eth2R2, interface eth1 via endIP_eth2R1, interface eth1 via endIP_eth3R1, interface eth0
----------------------------	--

b)

Aumentar o custo OSPF da interface **eth0 do SWL3A para 30**.

Aumentar o custo OSPF da interface **eth1 do SWL3A para 20**.

Aumentar o custo OSPF da interface **eth1 do Router 2 para 15**.

Caminho através da VLANs e Router 1: custo 20

Caminho através do SWL3A e Router 1: custo 25

Caminho através do SWL3A e Router 2: custo 35 por qualquer uma das duas hipóteses.

c)

Tabela de encaminhamento IPv6 do SWL3A:

C	redeVLAN1, diretamente ligada, interface vlan1	
C	redeVLAN2, diretamente ligada, interface vlan2	
C	redeVLAN3, diretamente ligada, interface vlan2	
C	redeDatacenter, diretamente ligada, interface eth1	
C	redeSWL3A-R2, diretamente ligada, interface eth0	
R	redeDMZ, [120/custo 1]	via endIP_eth3_Router2, eth0 via endIP_eth2_Router2, eth1 via endIP_eth2_Router1, eth1
R	redeR1-SWL3B, [120/custo 1]	via endIP_eth1_SWL3B, eth1 via endIP_eth2_Router1, eth1 via endIP_VLAN1_SWL3B, interface vlan1 via endIP_VLAN2_SWL3B, interface vlan2 via endIP_VLAN3_SWL3B, interface vlan3

(rota por omissão obtida por RIP)

R 0.0.0.0/0, [120/custo 1] via endIP_eth2R2, interface eth1
 via endIP_eth2R1, interface eth1
 via endIP_eth3R1, interface eth0

4.

C 210.1.1.128/27, directly connected, eth1
C 100.0.0.4/30, directly connected, eth0
B 195.5.5.0/25 [20/0], via 100.0.0.6, eth0

5)

NS		ns1.xptoinov.pt
MX	10	mail1.xptoinov.pt

ns1	A	endIPv4_DNS
ns1	AAAA	endIPv6_DNS
mail1	A	endIPv4_mail1
mail1	AAAA	endIPv6_mail1
http1	A	endIPv4_http1
http1	AAAA	endIPv6_http1

6)

i)

Colocar nas interfaces eth0 dos routers 1 e 2 (sentido de saída) uma ACL standard que negue o tráfego proveniente da VLAN 3:

```
access-list 1 deny IPv4Publico_VLAN3
access-list 1 deny IPv6_VLAN3
permit any
```

ii)

Colocar na interface VLAN 2 dos SWL3 A e B (sentido de entrada) uma ACL estendida que negue o tráfego proveniente da VLAN 2 e destinado ao servidor WEB do Datacenter:

```
access-list 101 deny IPv4Privado_VLAN2 IPv4Privado_Datacenter eq 80
access-list 101 deny IPv4Privado_VLAN2 IPv4Público_Datacenter eq 80
access-list 101 deny IPv6_VLAN2 IPv6_Datacenter eq 80
permit any any
```

7)

Se o browser suportar Web caching, isso permite: minimizar os tempos de resposta, minimizar o tráfego na rede. Assim, se um ficheiro está em cache no terminal, o browser faz um pedido com uma linha de cabeçalho do tipo *If-modified-since*. Se na cache estiver a última versão da página pedida, ela é imediatamente apresentada pelo terminal, caso contrário o servidor que a aloja será contactado.

8)

O POP3 corre sobre TCP e o número de porto do servidor é o 110 . A comunicação é estabelecida pela entidade (user agent) que pretende receber informação (pull protocol) . A transferência das mensagens é feita num de dois modos: envio-e-remoção: as mensagens são removidas da caixa de correio do servidor após serem enviadas ; envio-e-armazenamento: as mensagens são mantidas na caixa de correio após serem enviadas . O protocolo é executado em 3 fases:

- autenticação: o user agent envia o nome do utilizador e uma password
- transacção: o mail server envia as mensagens que estão na caixa de correio (mailbox) do utilizador; o user agent indica para cada mensagem, se deve ser removida ou não da caixa de correio
- actualização: o mail server remove da caixa de correio as mensagens indicadas pelo user agent para remoção

O IMAP corre sobre TCP e o número de porto do servidor é o 143 . Relativamente ao POP3, o IMAP permite ao utilizador funcionalidades adicionais importantes: (i) criar e gerir um sistema de directórios 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.

Numa sessão, o servidor está num de 4 estados:

- Estado não-autenticado: o estado inicial antes do user agent enviar o nome do utilizador e respectiva password
- Estado autenticado: o user agent deve identificar um directório antes de enviar qualquer comando que afecte as mensagens de correio
- Estado seleccionado: o user agent pode enviar comandos de gestão das mensagens (vizualizar, remover, transferir, etc...)
- Estado de saída (logout): quando a sessão termina