Dicas de Correção do Exame de Recurso de Redes e Serviços
31 de Janeiro de 2020

1a)

O switch/bridge raiz é o Switch 2, 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	10	4	1,2	3	A porta 3 está bloqueada porque o SW4 proporciona um percurso de custo menor para a raiz.
Switch 2	0	--	1,2,3	--	Switch raiz.
Switch 3	10	4	2,3	1	A porta 1 está bloqueada porque o SW4 proporciona um percurso de custo menor para a raiz.
Switch 4	5	3	1,2,4	--	Fornece o percurso de custo mínimo em todas as LANs a que está ligado.
Switch 5	15	4	1,5	2,3	Há três percursos de igual custo para a raiz, mas o SW3 é o que tem menor ID de entre todos os vizinhos nesses percursos.
SWL3 A	15	F1/0	--	F1/1	Não tem portas designadas porque nunca fornece o percurso de custo mínimo.
SWL3 B	15	F1/0	--	F1/1	Não tem portas designadas porque nunca fornece o percurso de custo mínimo.

1b)

Mudar o switch raiz para o SWL3A. Como este switch fornece ligação para a maior parte das redes IP da empresa, é mais eficiente que seja o switch raiz e o Default Gateway dos terminais das VLANs.

2a)
PÚBLICO:

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 VLAN 1 precisa de 10 IPv4 públicos, logo a sub-rede deverá ter um tamanho de 16 (10+2 routers+ID+Broadast=14 → 16); máscara /28.

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 16 (6+2 routers+ID+Broadast=10 → 16); máscara /28.

O NAT precisa de 6 IPv4 públicos, logo a sub-rede deverá ter um tamanho de 8 (6+ID+Broadast=8 → 8); máscara /29.

Fazendo subnetting da rede 194.4.4.128/25:

194.4.4.1xx/27, em que xx pode ser 00, 01, 10 ou 11, obtemos as seguintes subredes:

VLAN2	**191.1.1.128/27**
	194.4.4.160/27
	194.4.4.192/27
	194.4.4.224/27

Fazendo subnetting da rede 194.4.4.160/27:

194.4.4.101x/28, em que x pode ser 0 ou 1, obtemos as seguintes subredes:

VLAN1	**194.4.4.160/28**
DC	**194.4.4.176/28**

Fazendo subnetting da rede 194.4.4.192/27:

194.4.4.110x/28, em que x pode ser ou 1, obtemos as seguintes subredes:

DMZ	**194.4.4.192/28**
	194.4.4.208/28

Fazendo subnetting da rede 194.4.4.208/28:

194.4.4.1101x/29, em que x pode ser 0 ou 1, obtemos as seguintes subredes:

NAPT	**194.4.4.208/29**
Livre	**194.4.4.216/29**

Ainda fica mais uma rede livre:

Livre	**194.4.4.224/27**

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 10.10.0.0/16, pode-se usar qualquer IPv4 10.10.x.0/24.

VLAN1	10.10.1.0/24
VLAN2	10.10.2.0/24
VLAN3	10.10.3.0/24
Datacenter	10.10.4.0/24
DMZ	10.10.5.0/24
Rede SWL3A-R2	10.10.6.0/24
Rede SWL3B-R1	10.10.7.0/24
Rede SWL3A-R3	10.10.8.0/24
Old building	10.10.9.0/24

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

VLAN1	2001:2001:2001:1::/64
VLAN2	2001:2001:2001:2::/64
VLAN3	2001:2001:2001:3::/64
Datacenter	2001:2001:2001:4::/64
DMZ	2001:2001:2001:5::/64
Rede SWL3A-R2	2001:2001:2001:6::/64
Rede SWL3B-R1	2001:2001:2001:7::/64
Rede SWL3A-R3	2001:2001:2001:8::/64
Old building	2001:2001:2001:9::/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 A 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 → SW2 → SW1 → SWL3A). 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 e o ICMP Echo Request chega ao PC B. O Echo Reply fará o percurso PC B → SWL3 A → SW1 → SW2 → 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 SWL3A). 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 SWL3A.
Este switch 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 → SW1 → SW2 → PC A.

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!).

Vamos assumir que na redistribuição RIP → OSPF é usada uma métrica de 1.

Tabela de encaminhamento IPv4 do SWL3A
C rede DC, diretamente ligada, interface eth1
C rede R2_SWL3A, diretamente ligada, interface eth4
C redeR3-SWL3A, diretamente ligada, interface eth3
C rede VLAN1, diretamente ligada, interface VLAN1
C rede VLAN2, diretamente ligada, interface VLAN2
C rede VLAN3, diretamente ligada, interface VLAN3

R rede OldBuilding[120/1], via eth2R3, interface eth3
O rede DMZ [110/10], via eth3R2, interface eth2
via eth2R2, interface eth1
via eth2R1, interface eth1
O rede R1-SWL3B [110/10], via eth2R2, interface eth1
via eth1SWL3B, interface eth1

(rota por omissão obtida por RIP)
OE1 0.0.0.0/0, [110/15] , via eth3R2, interface eth2
via eth2R2, interface eth1
via eth2R1, interface eth1

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 RIP → OSPF é usada uma métrica de 1.

Tabela de encaminhamento IPv6 do Router1
C rede DC, diretamente ligada, interface eth2
C rede DMZ, diretamente ligada, interface eth1
C rede R1-RA, diretamente ligada, interface eth0
C rede R1-SWL3B, diretamente ligada, interface eth3

O rede SWL3A-R2[110/10], via eth1R2, interface eth1

O rede VLAN1[110/10], via eth2SWL3B, interface eth3
O rede VLAN2[110/10], via eth2SWL3B, interface eth3
O rede VLAN3[110/10], via eth2SWL3B, interface eth3

OE2 rede SWL3A-R3[110/11], via eth1R2, interface eth1
via eth1SWL3A, interface eth2
via eth2SWL3B, interface eth3
via VLAN1SWL3B, interface eth3
via VLAN2SWL3B, interface eth3
via VLAN2SWL3B, interface eth3

OE2 rede OldBuilding[110/11], via eth1R2, interface eth1
via eth1SWL3A, interface eth2
via eth2SWL3B, interface eth3
via VLAN1SWL3B, interface eth3

via VLAN2SWL3B, interface eth3
via VLAN2SWL3B, interface eth3

Não é preciso colocar a rota BGP para a rede exterior ao SA 1111.

c)

- Como as rotas anunciadas são 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.
- Assim, pode aumentar-se o custo dos interfaces eth1 do SWL3A, eth1 do SWL3B e eth2 do SWL3B para 10.

4.
i)
Colocar nas interfaces eth0 dos routers 1 e 2 (sentido de entrada) uma ACL extended que negue o protocolo tcp telnet para todos os endereços das redes IPv4 194.4.4.0/25 e IPv6 2001:2001:2001::/60:
access-list 101 deny tcp any 194.4.4.0 0.0.0.128 eq telnet
access-list 101 deny tcp any 2001:2001:2001::/60 eq telnet
access-list 101 permit ip any any
access-list 101 permit ipv6 any any

ii)
Colocar na interface eth1 do Router 3 (sentido de entrada) uma ACL extended que negue o tráfego destinado à DMZ (tanto em IPv4 como em IPv6):
access-list 102 deny ip redeOldBuilding redeDMZ
access-list 102 deny ipv6 redeOldBuilding redeDMZ
access-list 102 permit ip any any
access-list 102 permit ipv6 any any

5)

O atributo MED (Multi-Exit Discriminator) influencia a entrada no AS 1111. Logo, o Router 2 deve anunciar um valor de MED ao Router A superior ao que é anunciado pelo Router 1.

6)

a)
Os SAs representam um contrato entre dois peers e descrevem como é que eles irão usar os serviços de segurança IPSec para proteger o tráfego da rede. Um SA contém os seguintes parâmetros de segurança:

- Algoritmo de autenticação/cifra, tamanho da chave e outros parâmetros de cifra (e.g. tempo de vida da chave, ...)
- As chaves de sessão para autenticação e cifra, as quais podem ser introduzidas manualmente ou negociadas de forma automática
- Uma especificação do tráfego de rede ao qual o SA será aplicado (e.g. tráfego IP, sessões TELNET)
- Protocolo de encapsulamento IPSec AH ou ESP e modo túnel ou transporte

b)

Melhora o IPSec proporcionando características adicionais e flexibilidade; fornece autenticação para os peers IPSec, negoceia as chaves IPSec e negoceia as associações de segurança IPSec. O túnel IKE protege as negociações do SA. Depois dos SA estarem em funcionamento, o IPSec protege a transferência de informação. Vantagens:

- elimina a necessidade de especificar manualmente os parâmetros de segurança do IPSec em ambos os peers;
- permite que os administradores especifiquem um tempo de vida a a SA do IPSec;
- permite que as chaves de cifra mudem durante as sessões IPSec;
- permite que o IPSec forneça serviços anti-replay;
- permite suporte para certication authority (CA) no sentido de uma implementação escalável e de fácil gestão do IPSec;
- permite a autenticação dinâmica dos peers.

7)

i) O pacotes multicast começam a circular. Chegam ao R1 que os envia em flooding para R2, este faz a mesma coisa para R3 e R4. Como não há clientes ativos, R3 e R4 enviam *Prune* para R2, e este também enviar Prune para R1.
ii) Os PCs A e B enviam *IGMP Membership Report* a manifestar interesse em receber pacotes da sessão multicast. Os routers R3 e R4 enviam *Graft* para R2, que também envia *Graft* para R1. Os pacotes multicast passam a circular.
iii) O PC A envia um IGMP *Leave Group Report* para o Router 4. Este envia um *Prune* para R2. Só que o R3 ao ver o *Prune* terá que enviar um *Join* para continuar a receber pacotes multicast.
iv) O PC B envia um IGMP *Leave Group Report* para o Router 3. Este envia um *Prune* para R2, que por sua vez envia um *Prune* para R1. Os pacotes multicast deixam de circular.