Universidade de Aveiro
Licenciatura em Engenharia Informática

1ª parte do Exame de Redes e Serviços - 20 de janeiro de 2015

Duração: 1h30m. Sem consulta. Justifique cuidadosamente todas as respostas. Cotação: 20 valores.

1. Relativamente à rede de switches (SW1 a SW5, SWL3 A e SWL3B) da rede da empresa (SA 11) em anexo, considere que: (i) todas as ligações entre switches (layer 2-layer 2 ou layer 2-layer 3) são portas inter-switch/trunk, (ii) a ligação entre os swithes layer 3 é uma ligação layer 3 e (iii) o protocolo Spanning Tree está ativo em todos os switches/bridges.

a) Para o processo de Spanning-tree, indique e justifique qual o switch/bridge raiz, qual o custo de percurso para a raiz (root path cost) de cada switch/bridge, quais as portas raiz e quais as portas bloqueadas em cada switch/bridge. Justifique a sua resposta. Nota: a prioridade STP e o endereço MAC estão indicados junto ao respetivo switch/bridge e o custo STP de todas portas está entre parêntesis junto da respetiva porta. (4.0 valores)

b) Admitindo que nos últimos instantes existiu tráfego entre um terminal (A) ligado ao Switch 5 e um terminal (B) ligado ao Switch 4, escreva a tabela de encaminhamento do Switch 5? Notas: Identifique os endereços MAC de um equipamento por um identificador alfanumérico (ex: MACTerminalA). (1.5 valores)

c) Indique qual o switch mais adequado para ser a raiz do processo de Spanning-tree e porquê. E em caso de falha deste, qual deverá assumir o papel de raiz? Descreva possíveis alterações a efetuar nas configurações dos equipamentos de modo a garantir estes requisitos. Justifique convenientemente a sua resposta. (1.5 valores)

2. Considere a figura em anexo e os mesmos pressupostos da questão 1, mas onde são agora configuradas 3 VLANs em todos os switches. A empresa possui a gama de endereços IPv4 públicos 120.11.11.192/26 e vai usar a gama de endereços IPv4 privados 10.1.0.0/16. A empresa em questão possui ainda a gama de endereços IPv6 2200:11:11:1100::/60.

a) Defina sub-redes IPv4 públicas e/ou privadas (identificador e máscara) para todas as LAN e VLAN assumindo que existem serviços a correr em terminais/servidores que necessitam obrigatoriamente de endereços IPv4 públicos, nomeadamente: a VLAN 1 tem no máximo 10 terminais a necessitar de endereços públicos; o Datacenter necessita de 20 endereços públicos; os mecanismos de NAT/PAT necessitam de pelo menos 10 endereços públicos. (3.0 valores)

b) Defina sub-redes IPv6 (identificador e máscara) para todas as LAN e VLAN. (1.5 valores)

c) Atribua, onde necessário e apropriado, endereços IPv4 privados, IPv4 públicos e IPv6 aos terminais dos routers e switches layer 3. (1.5 valores)

d) Assumindo que um servidor DHCP (localizado no Datacenter) foi devidamente configurado e todas as configurações de rede relacionadas foram igualmente realizadas, descreva o processo de aquisição de um endereço IPv4 por um terminal ligado à VLAN 2 no Switch 1. (1.5 valores)

e) Considerando que as tabelas de ARP e de vizinhança IPv6 estão vazias, indique que pacotes são trocados (entre os equipamentos) e a sua sequência, quando efetua o comando *ping* IPv4 e um *ping* IPv6 a partir de um terminal da VLAN 1 ligado ao Switch 1 para um servidor no Datacenter (assuma que o *gateway* é o interface respetivo do SWL3 A). (1.5 valores)

3. Assumindo que os routers da rede da empresa da figura em anexo não têm qualquer protocolo de encaminhamento IPv4 ou IPv6 a correr. Como poderia garantir a conectividade IPv4 e IPv6 geral da rede (incluindo conectividade à Internet) usando apenas rotas estáticas. (2.0 valores)

4. Assuma que uma empresa adquiriu o domínio EmpresaX.pt e possui um servidor de DNS, dois servidores de email e dois servidores HTTP (WebMail, Webpage) numa rede com suporte IPv4 e IPv6. Defina diferentes nomes para os diferentes servidores/serviços e apresente uma configuração genérica da zona DNS (com todos os registos necessários) para o domínio EmpresaX.pt. Nota: identifique o endereço IP dos servidores por um identificador alfanumérico explícito (ex: IPV4servidorMail). (2.0 valores)

Universidade de Aveiro
Licenciatura em Engenharia Informática

2º Teste teórico/2ª parte do Exame de Redes e Serviços - 20 de janeiro de 2015

Duração: 1h30m. Sem consulta. Justifique cuidadosamente todas as respostas. Cotação: 20 valores.

1. Relativamente à rede da empresa (SA 11) em anexo considere considere que: (i) a ligação entre os switches layer 3 é uma ligação layer 3, (ii) estão configuradas 3 VLANs em todos os swithes e (iii) os Routers 1, 2 e switches layer 3 SWL3 A e B estão configurados com os protocolos de encaminhamento OSPFv2 e OSPFv3 (estando os custos das portas indicados entre parêntesis). Assuma ainda que o Router 1 está a anunciar uma rota por omissão.

a) Quais as tabelas de encaminhamento IPv4 e IPv6 do SWL3 A? Nota: Identifique as redes, endereços IP e nome dos interfaces por um identificador alfanumérico explícito (ex: redeIPv4VLAN1, endIPv4eth0Router1, intEth0Router1). (4.0 valores)

b) Pretende-se que qualquer pacote IP, com destino ao Datacenter, que chegue ao SWL3 A seja encaminhado preferencialmente através o interface eth1 do SWL3 B, em caso de falha deste pelo Router 1 e em último caso através dos interfaces VLAN do SWL3 B. Que configurações precisa de fazer para garantir este objetivo? Justifique devidamente a resposta. (2.0 valores)

2. Considere que os Routers 1 e A tem o protocolo BGP configurado e estabeleceram uma vizinhança entre os respetivos sistemas autónomos. Quais são os pacotes BGP trocados entre os Routers 1 e A após a configuração da vizinhança entre os sistema autónomos 11 e 22. (2.0 valores)

3. Considere o estabelecimento de uma sessão TCP sobre IPv4 entre um terminal (A) externo e um servidor (B) da empresa no Datacenter (com endereço IPv4 público). O servidor apenas aceita estabelecimento de ligações TCP no porto 80. Considere que o terminal A escolhe sempre como número de sequência inicial SN=5000 e o servidor B escolhe sempre SN=9000. Considere ainda que o comprimento máximo do campo de dados dos pacotes é 1500 octetos. Após o estabelecimento da sessão, um serviço em B entrega 4500 bytes para serem enviados a A, após o qual o terminal A termina a sessão estabelecida.

a) Desenhe um diagrama temporal que represente o conjunto de mensagens trocadas entre A e B, quando o terminal A tenta estabelecer um sessão TCP para o porto 80 do servidor B. Indique para cada mensagem as *flags* TCP ativas, o Sequence Number (SN) e o Acknowledgement Number (AN). (3.0 valores)

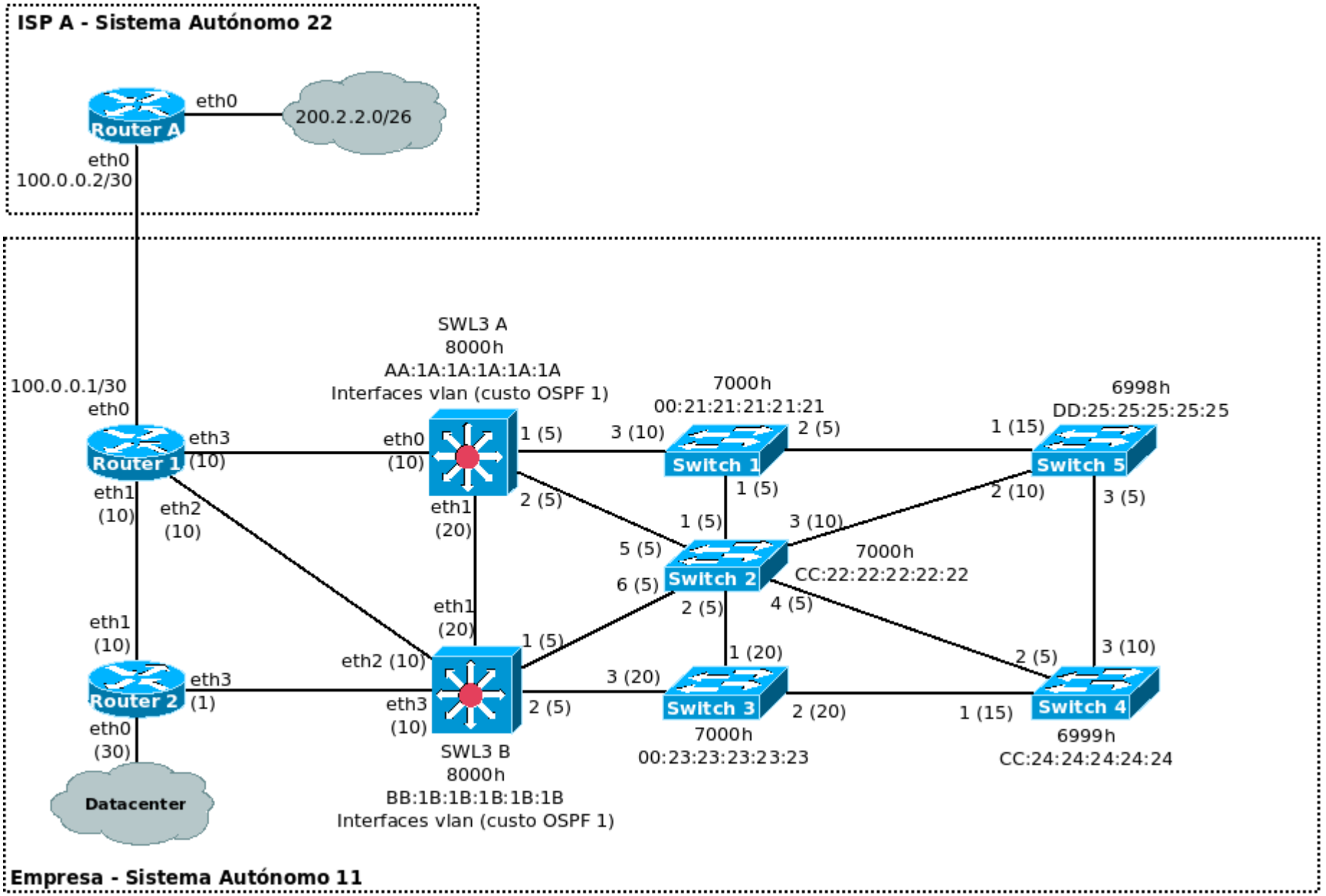
b) Desenhe um diagrama temporal que represente e identifique o conjunto de mensagens trocadas entre A e B, quando o terminal A tenta estabelecer um sessão UDP para o porto 80 do servidor B. (1.5 valores)

c) Ao monitorizar a rede do Datacenter observou-se um muito grande número de pacotes TCP com a *flag* RESET ativa do servidor B para o mesmo endereço IPv4 externo. Explique a origem do problema e proponha uma solução para o mesmo. (2.5 valores)

d) Indique como proceder para que um outro servidor (no Datacenter) com endereço IPv4 privado esteja acessível do exterior da rede da empresa. (1.5 valores)

4. A empresa da rede em anexo pretende criar um serviço de televisão interno sobre IP, para tal foi instalado no Datacenter um servidor de vídeo que emite 2 *streams* UDP (canais) de vídeo em contínuo. Identifique e descreva os mecanismos/protocolos a ativar nos routers de modo a que os *streams*/canais de vídeo possam chegar a múltiplos terminais de televisão IP espalhados pela rede. (2.0 valores)

5. Assumindo que todos os servidores do Datacenter possuem uma aplicação que notifica por rede a carga e ocupação de memoria do respetivo servidor usando UDP sobre IPv4 para o porto 3333 UDP de um servidor remoto. E que a mensagem é enviada em formato ASCII com a estrutura “dia, hora, ID_servidor, carga, memória”. Descreva genericamente uma possível arquitetura de uma aplicação (a correr num servidor remoto) que receba e registe as notificações de todos os servidores. (1.5 valores)


ISP A - Sistema Autónomo 22
Router A
eth0
200.2.2.0/26
eth0
100.0.0.2/30
Empresa - Sistema Autónomo 11
100.0.0.1/30
eth0
Router 1
eth3
(10)
eth1
(10)
eth2
(10)
SWL3 A
8000h
AA:1A:1A:1A:1A:1A
Interfaces vlan (custo OSPF 1)
eth0
(10)
1 (5)
2 (5)
eth1
(20)
7000h
00:21:21:21:21:21
3 (10)
2 (5)
Switch 1
1 (5)
6998h
DD:25:25:25:25:25
1 (15)
Switch 5
2 (10)
3 (5)
1 (5)
3 (10)
5 (5)
Switch 2
6 (5)
7000h
CC:22:22:22:22:22
2 (5)
4 (5)
eth1
(10)
Router 2
eth3
(1)
eth0
(30)
Datacenter
eth2 (10)
1 (5)
eth3
(10)
2 (5)
SWL3 B
8000h
BB:1B:1B:1B:1B:1B
Interfaces vlan (custo OSPF 1)
1 (20)
3 (20)
Switch 3
2 (20)
7000h
00:23:23:23:23:23
2 (5)
3 (10)
1 (15)
Switch 4
6999h
CC:24:24:24:24:24

Correção – Parte 1

1a)

O switch/bridge raiz é o Switch5, porque é o switch com o menor ID (menor prioridade 6998h).

	Custo para a raiz (RPC)	Porta raiz	Portas bloqueadas	Justificações
Switch 1	5	2	-	Ligação direta à raiz. A porta 2 é raiz, e as portas 1 (menor RPC em relação ao SW2) e 3 (fornece melhor caminho para a raiz do SWL3 A) são designadas.
Switch 2	10	3	1,4	Custo igual na ligação direta à raiz e no caminho via SW1. Prefere vizinho com menor ID (Raiz-SW5). Porta 3 é raiz, portas 2 (menor RPC em relação ao SW3), 5 (RPC igual mas menor ID em relação ao SWL3 A) e 6 (fornece melhor caminho para a raiz ao SWL3 B) são designadas. Portas 1 (maior RPC em relação ao SW1) e 4 (RPC igual, maior ID em relação ao SW4) bloqueiam.
Switch 3	30 (20+10)	2	1,3	Custo igual no caminho via SW2 e no caminho via SW4. Prefere vizinho com menor ID (SW4). Porta 2 é raiz, portas 1 e 3 bloqueiam (maior RPC em relação aos vizinhos).
Switch 4	10	3	-	Ligação direta à raiz. Porta 3 é raiz, portas 1 (fornece melhor caminho para a raiz ao SW3) e 2 (RPC igual mas menor ID em relação ao SW2) são designadas.
Switch 5	-	-	-	-
SWL3 A	10 (5+5)	1	2	Caminho de menor custo via SW1. Porta 1 é raiz, porta 2 bloqueia (RPC igual mas maior ID em relação ao SW2) .
SWL3 B	15 (5+10)	1	-	Custo igual no caminho via SWL3 A e no caminho via SW2. Prefere vizinho com menor ID (SW2). Porta 1 é raiz, porta 2 é designada (RPC menor em relação ao SW3).

1b)
Tabela de encaminhamento Layer 2 (forwarding table) do SW5.

Endereço MAC	**Porta (do próprio switch)**
MAC_terminalA	4 (assumindo que o terminal está nesta porta)
MAC_terminalB	3 (porta que liga ao SW4, de onde vem o tráfego do terminal B).
MAC_SW1	1 (MAC aprendido com os pacotes da Spanning-tree)
MAC_SW2	2 (MAC aprendido com os pacotes da Spanning-tree)
MAC_SW4	3 (MAC aprendido com os pacotes da Spanning-tree)

1c) Os SWL3 A ou B deverão ser a raiz porque são os que fazem a agregação do tráfego das VLAN em direção ao centro da rede e Internet. Assumindo que a primeira raiz é o A e a secundário o B, então a prioridade da do SWL3A deverá ser a menor de todos os switches e a prioridade do B a segunda menor.

2a) e b)
A VLAN1 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 Datacenter precisa de 20 IPv4 públicos, logo a sub-rede deverá ter um tamanho de 32 (20+1 routers+ID+Broadast=23 → 32); máscara /27.

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

Começando da rede maior e a partir de 120.11.11.192/26:

Datacenter	120.11.11.192/27	(+32 endereços)
VLAN1	120.11.11.224/28	(+16 endereços)
NAT	120.11.11.240/28	

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 10.1.0.0/16, pode-se usar qualquer IPv4 10.1.X.X. Logo as LANs podem ter a rede 10.1.X.0/24 com X de 0 a 255.

A rede IPv6 disponível é 2200:11:11:1100::/60 logo pode-se definir qualquer endereço que comece por 2200:11:11:110X: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 2200:11:11:110X::/64 com X de 0 a F.

Possível solução:

VLAN1	10.1.1.0/24	2200:11:11:1101::/64
VLAN2	10.1.2.0/24	2200:11:11:1102::/64
VLAN3	10.1.3.0/24	2200:11:11:1103::/64
Datacenter	10.1.200.0/24	2200:11:11:1100::/64
Rede SWA-SWB	10.1.100.0/30	2200:11:11:1104::/64
Rede R1-SWA	10.1.100.4/30	2200:11:11:1105::/64
Rede R1-SWB	10.1.100.8/30	2200:11:11:1106::/64
Rede R1-R2	10.1.100.12/30	2200:11:11:1107::/64
Rede R2-SWB	10.1.100.16/30	2200:11:11:1108::/64

2c)
De cada rede não se pode usar o identificador (primeiro endereço) nem o broadcast (último endereço).
Possível solução

		IPv4 público	IPv4 privado	IPv6
Router1	**eth1**	-	10.1.100.13	2200:11:11:1107::1
Router1	**eth2**	-	10.1.100.9	2200:11:11:1106::1
Router1	**eth3**	-	10.1.100.5	2200:11:11:1105::1
Router2	**eth0**	120.11.11.193	10.1.200.1	2200:11:11:1100::1
Router2	**eth1**	-	10.1.100.14	2200:11:11:1107::2
Router2	**eth3**	-	10.1.100.17	2200:11:11:1108::1
SWL3 A	**eth0**	-	10.1.100.6	2200:11:11:1105::2
SWL3 A	**eth1**	-	10.1.100.1	2200:11:11:1104::1
SWL3 A	**vlan1**	120.11.11.225	10.1.1.1	2200:11:11:1101::1
SWL3 A	**vlan2**	-	10.1.2.1	2200:11:11:1102::1
SWL3 A	**vlan3**	-	10.1.3.1	2200:11:11:1103::1
SWL3 B	**eth1**	-	10.1.100.2	2200:11:11:1104::2
SWL3 B	**eth2**	-	10.1.100.10	2200:11:11:1106::2
SWL3 B	**eth3**	-	10.1.100.18	2200:11:11:1108::2
SWL3 B	**vlan1**	120.11.11.226	10.1.1.2	2200:11:11:1101::2
SWL3 B	**vlan2**	-	10.1.2.2	2200:11:11:1102::2
SWL3 B	**vlan3**	-	10.1.3.2	2200:11:11:1103::3

2d)
Como o servidor de DHCP está no Datacenter então todos os routers/SWL3 vão ter de redirecionar os pedidos para o servidor (servindo de intermediários). Para esse efeito é preciso configurar todos os routers como BOOTP Relay Agents.
Um terminal que deseje obter um endereço IP irá enviar um pacote DHCP DISCOVER em broadcast, que chegará a um router o qual incluirá no pacote o endereço IPv4 onde recebeu o pacote (para o servidor DHCP poder identificar a rede de origem) e reenviará em unicast o DISCOVER para o servidor, o servidor perante este pedido identifica a rede de origem e procurará na gama de endereços dessa rede um disponível, reenviará a oferta num pacote DHCP OFFER já com o endereço via routers para o terminal, o terminal responderá com um DHCP REQUEST ao qual o servidor (se tudo estiver de acordo com o oferecido) enviará um DHCP ACKNOWLEDGEMENT.

2e) 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 responderá com um ARP REPLY. Depois o terminal constrói o cabeçalho Ethernet e envia um pacote IP com um pacote ICMP ECHO-REQUEST. 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.

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/REPLAY são pacotes ICMPv6.

3. Com rotas estáticas para as redes que cada equipamento desconhece e uma rota por omissão para a Internet.

SWL3 A:
Rede R1-SWL3B, via endIP_eth1_SWL3B
Rede R2-SWL3B, via endIP_eth1_SWL3B
Rede R1-R2, via endIP_eth3_R1
Rede Datacenter, via endIP_eth3_R1
Rota por omissão, via endIP_eth3_R1

SWL3 B:
Rede R1-SWL3A, via endIP_eth1_SWL3A
Rede R1-R2, via endIP_eth3_R2
Rede Datacenter, via endIP_eth3_R2
Rota por omissão, via endIP_eth3_R2

R2:
Redes VLANs, via endIP_eth3_SWL3B
Rede R1-SWL3B, via endIP_eth3_SWL3B
Rede R1-SWL3A, via endIP_eth1_R1
Rede SWL3A-SWL3B, via endIP_eth3_SWL3B
Rota por omissão, via endIP_eth1_R1

R1:
Redes VLANs, via endIP_eth0_SWL3A
Rede R2-SWL3B, via endIP_eth1_R2
Rede Datacenter, via endIP_eth1_R2
Rede SWL3A-SWL3B, via endIP_eth0_SWL3A
Rota por omissão EXTERNA, via endIP_eth0_RA

4.
Servidor DNS, v, endIPv6_DNS
Servidor mail 1, endIPv4_mail1, endIPv6_mail1 (nome: mail1.empresax.pt)
Servidor mail 2, endIPv4_mail2, endIPv6_mail2 (nome: mail2.empresax.pt)
Servidor HTTP 1, endIPv4_http1, endIPv6_http1 (nome: webmail.empresax.pt)
Servidor HTTP 2, endIPv4_http2, endIPv6_http2 (nome: webpage.empresax.pt)

DNS:
empresax.pt **NS** ns1.empresax.pt
empresax.pt **MX** 10 mail1.empresa.pt
empresax.pt **MX** 20 mail2.empresa.pt

ns1 **A** endIPv4_DNS
ns1 **AAAA** endIPv6_DNS
mail1 **A** endIPv4_mail1
mail1 **AAAA** endIPv6_mail1
mail2 **A** endIPv4_mail2
mail2 **AAAA** endIPv6_mail2

webmail **A** endIPv4_http1
webmail **AAAA** endIPv6_http1
webpage **A** endIPv4_http2
webpage **AAAA** endIPv6_http2

Correção – Parte 2

1a)
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!).

Tabela de encaminhamento SWL3A
C redeVLAN1, diretamente ligada, interface vlan1
C redeVLAN2, diretamente ligada, interface vlan2
C redeVLAN3, diretamente ligada, interface vlan2
C redeR1-SWL3A, diretamente ligada, interface eth0
C redeSWL3B-SWL3A, diretamente ligada, interface eth1

O redeR1-SWL3B, [custo 11] via endIP_intVLAN1_SWL3B, interface vlan1
via endIP_intVLAN2_SWL3B, interface vlan2
via endIP_intVLAN3_SWL3B, interface vlan3
O redeR2-SWL3B, [custo 11] via endIP_intVLAN1_SWL3B, interface vlan1
via endIP_intVLAN2_SWL3B, interface vlan2
via endIP_intVLAN3_SWL3B, interface vlan3
O redeR1-R2, [custo 20] via endIP_eth3_R1, interface eth0
O rede Datacenter, [custo 41] via endIP_intVLAN1_SWL3B, interface vlan1
via endIP_intVLAN2_SWL3B, interface vlan2
via endIP_intVLAN3_SWL3B, interface vlan3

(rotas por omissão obtidas por OPSF)
IPv4 → O 0.0.0.0/0, via endIPv4_eth3R1, interface eth0
IPv6 → O ::/0, via endIPv6_eth3R1, interface eth0

Nota: os interfaces LAYER 3 das VLAN (int vlan1, vlan2, vlan3) tinham custo 1, logo os caminhos mais curtos eram sempre via VLANs.

1b)
O caminho para o Datacenter via SWL3B tem um custo de 60, via R1 um custo de 50 e via VLANs um custo de 41.
Para garantir os requisitos é preciso alterar os custos do OSPF de modo a garantir que o primeiro caminho tem o menor custo de todos e o segundo o segundo menor custo.
Possível solução:
Aumentar o custo dos interfaces VLAN do SWL3A para 100 e aumentar o custo do do interface eth0 do SWL3A para 30. Assim os custos para o Datacenter ficam: via SWL3B tem um custo de 60, via R1 um custo de 70 e via VLANs um custo de 140.

2.
Após a configuração da relação de vizinhança os routers estabelecem um sessão TCP e trocam os pacotes BGP OPEN (para definir os parâmetros da vizinhança), UPDATE (para anunciar as redes) e KEEPALIVE (para manter a relação/sessão aberta).

Nota: os pacotes BGP NOTIFICATION só são enviados em caso de erro.

3 a)

Terminal A	**Servidor B**
Abertura da sessão:	
TCP [SYN], SN=5000, AN=0 →	
	←TCP [SYN,ACK], SN=9000, AN=5001
TCP [ACK], SN=5001, AN=9001 →	
Troca de dados:	
	←TCP [ACK, 1500 bytes], SN=9001, AN=5001
TCP [ACK], SN=5001, AN=10501 →	←TCP [ACK, 1500 bytes], SN=10501, AN=5001
TCP [ACK], SN=5001, AN=12001 →	←TCP [ACK, 1500 bytes], SN=12001, AN=5001
TCP [ACK], SN=5001, AN=13501 →	
Finalização:	
TCP [FIN], SN=5001, AN=13501 →	
	←TCP [ACK], SN=13501, AN=5002
	←TCP [FIN], SN=13501, AN=5002
TCP [ACK], SN=5001, AN=13502 →	

3b)

UDP, porto destino 80 →	**PORTO UDP 80 ESTÁ FECHADO!**
	←ICMP PORT UNREACHABLE (port 80)

3c)
Um pacote TCP com a flag RESET ativa é enviado em resposta a um pacote TCP com a flag SYN ativa recebido num porto TCP fechado (o porto TCP 81 está fechado, só o 80 está aberto!).
O número elevado de pacotes com a flag RESET ativa indica que está a ser tentado o estabelecimento de muitas sessões TCP para portos (serviços) fechados no servidor. Para resolver o problema é preciso bloquear os pacotes TCP (com flag SYN ativa) que vêm de fora da rede ativando na firewal da rede (ou no Router 1) uma regra (ACL) que negue a passagem de tráfego proveniente do endereço IP exterior em questão.

Nota: Isto pode ser o resultado de um ataque de negação de serviço para bloquear o servidor ou um port-scan (procura ativa de serviços nos servidores).

3d) Assumindo que os mecanismos de NAT/PAT já estão ativos (se não estiverem é preciso ativá-los), é preciso configurar uma associação estática de NAT/PAT que associe de forma permanente um endereço IP público ao endereço IP privado do servidor.

Nota: O NAT/PAT só começa a tradução de endereços de comunicações quando estas são iniciadas do interior da rede!

4. É preciso ativar o encaminhamento multicast nos routers. Para isso é preciso ativar o protocolo IGMP para receber os pedidos de adesão/saída dos terminais aos grupos multicast, e ativar um protocolo de encaminhamento que troque informação entre os routers de como encaminhar os pacotes multicast (possíveis protocolos: PIM Sparse-mode, Pim Dense-mode, MOSPF, DVMRP).

5. A aplicação do servidor necessita de ter um SOCKET UDP (aberto no porto 3333) para receber os pacotes UDP com a informação. A aplicação deverá então depois ter um ciclo que: 1. espere por um pacote, 2. receba o pacote. 3. leia e processe os conteúdos do pacote, 4. escreva a informação num ficheiro ou BD, voltar a 1 para receber/processar o pacote seguinte.