Exame de 24 de Junho de 2015
Dicas de resolução

1a)

IPv4 privado:

Cada VLAN local pode ter até 256 terminais (>254), logo a rede deverá ter pelo menos uma máscara de /23 (510 endereços usáveis). A VLAN end-to-end pode ter até 300 terminais (>254), logo a rede deverá ter pelo menos uma máscara de /23 (510 endereços usáveis).

Precisamos assim de 5 VLANs com máscara /23.
10.10.0.0/23 -VLAN1
10.10.2.0/23 -VLAN2
10.10.4.0/23 -VLAN3
10.10.6.0/23 -VLAN4
10.10.8.0/23 -VLAN end-to-end

O Datacenter precisa de 24 endereços privados, logo a rede deverá ter pelo menos uma máscara de /27 (30 endereços usáveis).
10.10.10.0/27 – DMZ
10.10.10.32/27 – redes ponto-a-ponto

As ligações ponto a ponto poderão ter uma máscara /30 (2 endereços usáveis).

Router2-SWL3 E	10.10.10.34/30
Router2-Router3	10.10.10.36/30
Router3-SWL3 E	10.10.10.38/30
SWL3E-Datacenter	10.10.10.40/30
VLAN de Interligação	10.10.10.48/28

IPv4 público:

20.15.15.0/25 – VLAN 1 (que necessita de 80 endereços públicos), logo a rede deverá ter pelo menos uma máscara de /25 (126 endereços usáveis).
20.15.15.128/26 – Datacenter (que necessita de 24 endereços públicos), logo a rede deverá ter pelo menos uma máscara de /27 (30 endereços usáveis).
20.15.15.192/26 – NAT

IPv6 global:

Como a máscara de rede é /52, os primeiros 52 bits são fixos e apenas os 12 bits até à máscara de /64 podem ser usados. Em VLANs para que os mecanismos stateless de atribuição de endereços funcionem, a máscara tem que ser /64. Nas ligações ponto-a-ponto pode usar-se outra máscara.

2000:AA:AA:0XXX::/64, com XX a variar de 000h até FFFh.

1b)
Devemos colocar um ou dois SWL3 no Datacenter e um ou dois SWL3 no Edifício Antigo, todos ligados ao SWL3E através de ligações trunk/inter-switch que transportam a VLAN end-to-end. Deve ser criada uma VLAN de interligação entre cada um destes edifícios e o SWL3 E do core. A VLAN end-to-end deve ser configurada como passiva.

1c)
Colocar mais um SWL3 no core, ligado ao SWL3 E. Da distribuição para este SWL3 deve ser criada uma nova VLAN de interligação.
Os switches L2 de cada piso devem ser ligados aos 2 swicthes L3 do respetivo piso.
Colocar mais um router de acesso à Internet, ligado ao Router 2, ao SWL3 E e ao Router 3.
Eventualmente as saídas do Edifício Antido e do Datacenter também poderiam ter dois Routers ou SWL3 de saída, ligando ao core.

1d)
A empresa deverá ter dois servidores DNS, um público e um privado.
O **servidor privado** deve estar localizado numa rede sem acesso do exterior e ligada à camada de core, de modo a minimizar o tempo médio de acesso por parte de todos os equipamentos da rede.
O **servidor público** deve estar localizado numa rede com acesso a partir do exterior e o mais próxima possível dos routers do ISP, como por exemplo a DMZ.

O servidor DNS **público** contém registos do tipo A, que permitem fazer a tradução de um nome num endereço IPv4 das máquinas com endereços públicos, registo do tipo AAAA, que permitem fazer a tradução de um nome num endereço IPv6 das máquinas com endereços globais. Contém ainda um registo NS que identifica o nome do servidor DNS público, um registo do tipo A que identifica o endereço IPv4 do servidor DNS público a partir do nome e um registo AAAA que identifica o endereço IPv6 do servidor DNS público a partir do nome.

O servidor DNS **privado** contém todos os registos do servidor público e ainda todos os registos do tipo A para todas as máquinas com endereços privados.

1e)
No servidor de DHCP localizado no Datacenter é preciso configurar uma pool de endereços para cada uma das VLAN, em que se atribui o endereço IP, a máscara de sub-rede, o default gateway, entre outras possíveis configurações. Das gamas configuradas deverão ser excluídos os endereços IP configurados manualmente nos routers/switches/servidores.
Depois é necessário configurar em cada interface VLAN dos SWL3 A a E o DHCP BOOTP Relay Agent, para que os pedidos DHCP de cada VLAN possam passar para o Datacenter e o servidor saiba a que rede IP (VLAN) correspondem os pedidos.

2a)
Tabela encaminhamento IPv4

C Rede_VLANInter, diretamente ligada
C Rede_SWL3E-Router2, diretamente ligada
C Rede_SWL3E-Router3, diretamente ligada
C Rede_SWL3E-Datacenter, diretamente ligada

R RedeVLAN1, custo 1, via ipVLANInterSWL3A, trunk_SWL3E
custo 1, via ipVLANInterSWL3B, trunk_SWL3E
R RedeVLAN2, custo 1, via ipVLANInterSWL3A, trunk_SWL3E
custo 1, via ipVLANInterSWL3B, trunk_SWL3E
R RedeVLAN3, custo 1, via ipVLANInterSWL3C, trunk_SWL3E
custo 1, via ipVLANInterSWL3D, trunk_SWL3E
R RedeVLAN4, custo 1, via ipVLANInterSWL3C, trunk_SWL3E
custo 1, via ipVLANInterSWL3D, trunk_SWL3E
R Rede_Router2_Router3, custo 2, via ipRouter2, interSWL3E_Router2
custo 2, via ipRouter3, interSWL3E_Router3

R 192.168.5.0/24, custo 6, via ipRouter2, int_SWL3E_R2
R 0.0.0.0/0, custo11, via ipRouter3, int_SWL3E_R3

Em relação à VLAN end-to-end, há duas possibilidades: se esta VLAN for configurada no SWL3E, aperece como local:

C Rede_VLANEndtoEnd, diretamente ligada

senão aparecem quatro caminhos diferentes:

R RedeVLANEndtoEnd, custo 1, via ipVLANInterSWL3A, trunk_SWL3E
custo 1, via ipVLANInterSWL3B, trunk_SWL3E
custo 1, via ipVLANInterSWL3C, trunk_SWL3E
custo 1, via ipVLANInterSWL3D, trunk_SWL3E

Tabela encaminhamento IPv6
--
C Rede_VLANInter, diretamente ligada
C Rede_SWL3E-Router2, diretamente ligada
C Rede_SWL3E-Router3, diretamente ligada
C Rede_SWL3E-Datacenter, diretamente ligada

R RedeVLAN1, custo 1, via ipVLANInterSWL3A, trunk_SWL3E
custo 1, via ipVLANInterSWL3B, trunk_SWL3E
R RedeVLAN2, custo 1, via ipVLANInterSWL3A, trunk_SWL3E
custo 1, via ipVLANInterSWL3B, trunk_SWL3E
R RedeVLAN3, custo 1, via ipVLANInterSWL3C, trunk_SWL3E
custo 1, via ipVLANInterSWL3D, trunk_SWL3E
R RedeVLAN4, custo 1, via ipVLANInterSWL3C, trunk_SWL3E
custo 1, via ipVLANInterSWL3D, trunk_SWL3E

R Rede_Router2_Router3, custo 2, via ipRouter2, interSWL3E_Router2
custo 2, via ipRouter3, interSWL3E_Router3
--
R ::/0, custo11, via ipRouter3, int_SWL3E_R3

Em relação à VLAN end-to-end, há duas possibilidades: se esta VLAN for configurada no SWL3E, aperece como local:

C Rede_VLANEndtoEnd, diretamente ligada

senão, existem 4 caminhos diferentes:

R RedeVLANEndtoEnd, custo 1, via ipVLANInterSWL3A, trunk_SWL3E
custo 1, via ipVLANInterSWL3B, trunk_SWL3E
custo 1, via ipVLANInterSWL3C, trunk_SWL3E
custo 1, via ipVLANInterSWL3D, trunk_SWL3E

2b)
O terminal envia um ARP Request na VLAN end-to-end e por isso, esse pacote chega através do trunk a todos os switches do piso 2 (SWL3A ou SWL3B->SWL3E->SWL3C e SWL3D). O terminal destino irá responder com um ARP Response que chegará ao SWL3 do piso A de onde seguiu o ARP Request. Seguidamente, o ICMP Echo Request será enviado para o SWL3A (vamos supor) e chegará a todos os SWL3. O Echo Reply fará o percurso inverso, através dos trunks. Note-se que todos estes pacotes são encapsulados de acordo com o protocolo IEEE 802.1Q, que suporta as ligações interswitch.

Para o Datacenter a situação é diferente. O terminal enviará o ARP Request para o Default Gateway (SWL3A, vamos supor). O SWL3 A vai responder (ARP Reply) e depois o terminal enviará o ICMP Echo Request para o SWL3 A. Este irá consultar a sua tabela de encaminhamento e verificará que tem que enviar o pacote através da VLAN de interligação, em direção ao SWL3 E. Há uma troca de ARP Request e ARP Reply para que o SWL3A descubra o MAC address do next-hop, e o ICMP Echo Request é enviado para o SWL3 E. Este verifica que tem que enviar para a rede do Datacenter e efetua nova troca de ARP Request e ARP Reply para descobrir o MAC address do destino. Finalmente, o ICMP Echo Request chega ao destino. Na resposta, o ICMP Echo Reply fará o percurso inverso.

2c)
A DMZ terá políticas de segurança menos restritivas. A melhor localização será ligada ao Router 3 ou ao SWL3 E. Através de ACLs específicas, será possível criar uma política de segurança apropriada.

2d)
Podemos configurar uma ACL estendida, em que se identifica a origem (IP da VLAN end-to-end) e do destino (rede IP do Datacenter). Uma vez que a VLAN sem fios é end-to-end, a ACL deveria ser colocada em todos os SWL3 dos pisos.

3)
Configuração do SNMP em todos os equipamentos da rede, que passarão a ser agentes SNMP, e definição de comunidades. Através de um script, é possível ler a informação das MIBs dos equipamentos, nomeadamente as suas tabelas ARP. Esta monitorização deve ser feita recorrendo a uma VLAN end-to-end. Depois será feito um pós-processamento que irá verificar se existe mais do que um MAC address associado ao mesmo endereço IP, o que será sinal de existir um ataque de IP spoofing. A máquina responsável pelo pooling dos equipamentos SNMP e pelo pós-processamento deverá estar colocada preferencialmente no Datacenter.

4)
Política de QdS baseada na arquitetura DiffServ.
Em primeiro lugar, temos que definir as classes de tráfego, como por exemplo: classe EF para o tráfego de vídeo e classe Default para o restante tráfego.
Os routers fronteira (SWL3 A-E) são responsáveis pela marcação dos pacotes no campo DSCP (nos seus interfaces de entrada), neste caso com o valor 46 correspondente à classe EF ou 0 para a classe DE. Nos interfaces de saída são aplicadas políticas de QdS apropriadas (por exemplo, atribuindo uma percentagem de LB adequada a cada uma das classes de tráfego).
A identificação dos pacotes é normalmente feita recorrendo a ACLs.

5)
Criar no Router 3 uma rota por omissão para o Router do ISP2 e definir uma métrica (distância administrativa) superior à rota que existe para o ISP1. Desta forma, esta segunda rota será uma rota por omissão flutuante (*floating static route*).

6a)
- a fonte S começa a enviar pacotes multicast para o SWL3 E, que os encaminha para todos os seus trunks e interfaces L3;
- estes pacotes chegam a todos os SWL3 A-D e aos routers R2 e 3;
- os switches L3 de cada piso trocam ASSERT para decidir quem continua a encaminhar os pacotes multicast;
- supondo que o terminal R está ligado ao SWL3 C, os switches L3 A, B e D, bem como os routers 2 e 3 irão enviar mensagens PIM PRUNE ao longo dos seus interfaces RPF para não continuarem a receber os pacotes multicast;
- o SWL3 C também enviar pacotes PIM PRUNE no seus interfaces que não são RPF;
- o SWL3 E deixa de encaminhar pacotes multicast nos trunks que ligam aos SWL3 A, B e D, bem como nos interfaces que ligam aos routers 2 e 3.

6b)
- O terminal enviará um IGMP Membership Report ao SWL3 A (supondo que está ligado a ele) para indicar que pretende aderir ao grupo multicast IPv4 234.234.234.234.

- o SWL3 A irá enviar uma mensagem PIM JOIN para o SWL3 E;
- o SWL3 E passa a enviar os pacotes multicast no trunk que o liga ao SWL3 A.

6c)
O – S
G – 234.234.234.234
E – interface SWL3 E – Datacenter
S1 - interface trunk SWL3 E – SWL3 A (por exemplo)
S2 - interface trunk SWL3 E – SWL3 C (por exemplo)