PROTOCOLOS DE COMUNICAÇÃO
EXAME DE ÉPOCA DE RECURSO
2024-07-05

RESOLUÇÃO ESQUEMÁTICA

1. Utilizamos serviços cada vez mais sofisticados, que recorrem à inteligência artificial e à aprendizagem máquina, e que exigem o processamento de quantidades massivas de dados bem como redes com cada vez maior desempenho. Do ponto de vista dos protocolos de comunicação, quais são as principais soluções para esses desafios?

Soluções

20% - mecanismos de controlo de congestão mais eficazes
20% - protocolos com multi-homing / multipath
20% - suporte de QoS – reserva de recursos para fluxos ou classes
20% - redes definidas por software (SDN)→ melhor e maior controlo de recursos, QoS, escalabilidade e segurança
20% - virtualização de funções de rede (NFV) → escalabilidade, dinamismo, partilha de recursos, cloud

2. Descreva as principais características do protocolo QUIC e explique a razão da importância dessas características. Quais as vantagens do protocolo QUIC face ao protocolo TCP? Como é que o QUIC atravessa os servidores de NAT e como resolve o problema de NAT-rebinding?

35% Protocolo QUIC – Principais características
- segurança embutida – reduz a latência no estabelecimento de ligações HTTP
- multistreaming – elimina o head of line blocking
- multipath – tira partido de múltiplas ligações simultâneas, o que é frequente nos dispositivos atuais

35% Vantagens face ao TCP
- Estabelecimento mais rápido de ligações, com vantagens para o tráfego HTTP
- Não tem HoL blocking

30% QUIC e NAT
- funcionamento sobre UDP – faz com que o protocolo seja compatível com NAT
- ID de ligação - permite resolver o problema do NAT re-binding

3. O sobredimensionamento das redes resolve o problema do fornecimento de qualidade de serviço adequada às aplicações? Justifique. Que outras formas conhece para garantir que a rede Internet, desenhada para funcionar em modo 'best effort', consiga ser utilizada por aplicações que tenham requisitos específicos de qualidade de serviço?

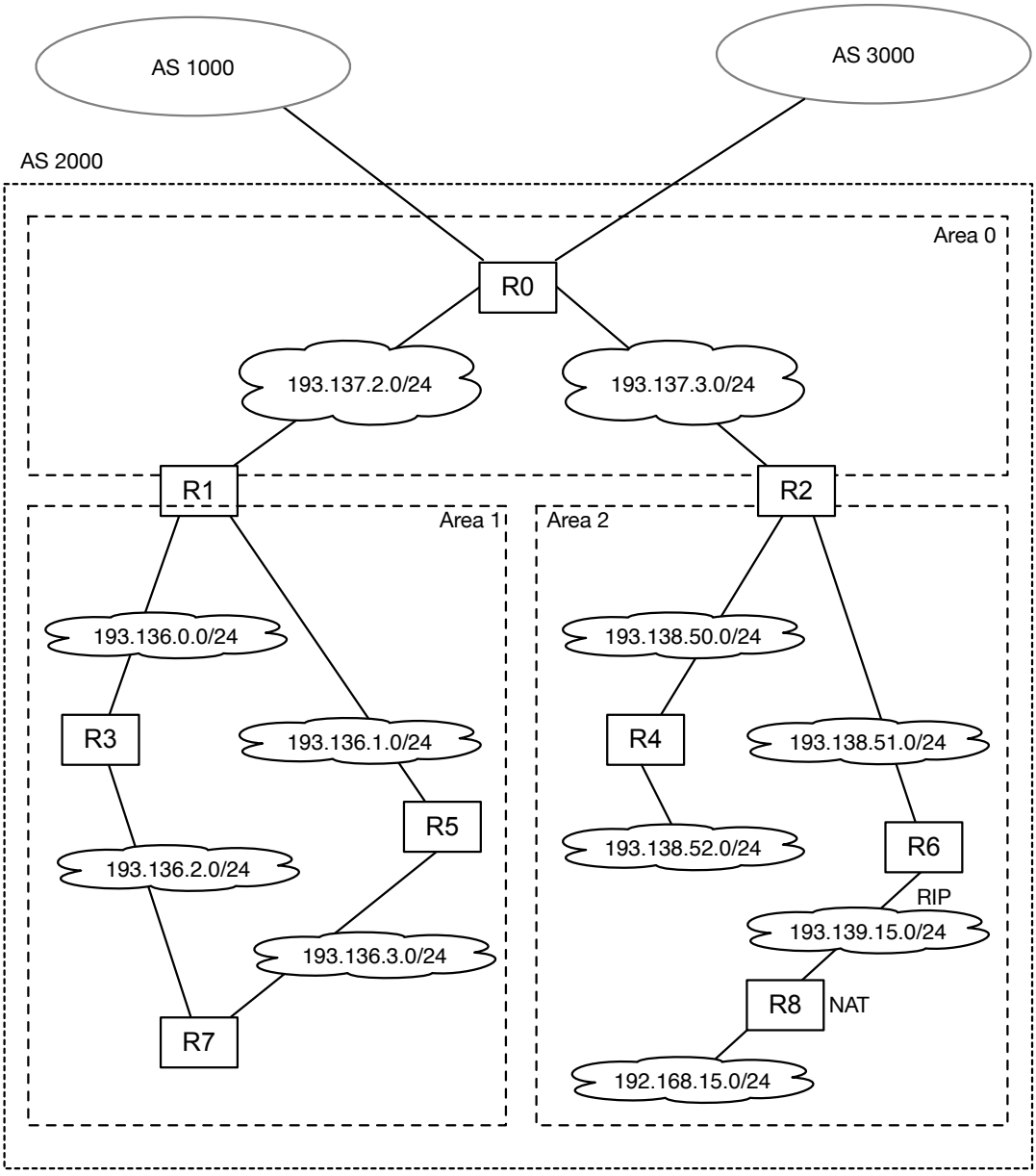
- 25% **Sobredimensionamento**
  - Resolve o problema do fornecimento de QoS, dado que estão sempre disponíveis os recursos necessários, não havendo congestionamento;
  - No entanto, não é viável do ponto de vista económico nem de um ponto de vista prático.

- **Outras formas**
  - 25% IntServ – não escalável nem viável em redes com muitos fluxos
  - 25% DiffServ – exige reserva de recursos para classes; não dá garantias fim-a-fim;
  - 25% SDN – engenharia de tráfego, encaminhamento, reserva de recursos, controlo de admissão, etc.

4. Nas redes definidas por software (Software-Defined Networks, SDN) como é feito o encaminhamento de pacotes? Se, neste tipo de redes, for detetado um ataque de DoS (Denial of Service) a determinado servidor, o que pode ser feito? É possível utilizar os conceitos de SDN e NFV (Network Function Virtualization) separadamente? Porquê?

   35% **Encaminhamento de pacotes** – os caminhos são decididos centralmente no controlador, usando um algoritmo de encaminhamento; são, depois, instalados nas flow tables de cada switch ao longo do caminho
   35% **Deteção de ataque de DoS** – após deteção, as flows table dos diversos switchs ao longo do caminho são alteradas, de modo a eliminar os pacotes do fluxo atacante
   30% **SDN e NFV** – são conceitos distintos (explicar) e, portanto, podem ser implementados independentemente. A conjugação dos dois conceitos permite tirar partido das vantagens de cada um deles, pelo que é desejável e bastante frequente.

5. Considere o cenário apresentado abaixo. Para esse cenário, apresente:



a) a configuração de encaminhamento do router R1, sabendo que nas áreas 0 e 1 só é usado o protocolo OSPF de encaminhamento interior e que todas as redes da área 1 devem ser anunciadas para o exterior da área como uma única rede /21;

20%

```
router ospf 100
    network 193.137.2.0 0.0.0.255 area 0
    network 193.136.0.0 0.0.0.255 area 1
    network 193.136.1.0 0.0.0.255 area 1
    area 1 range 193.136.0.0 255.255.248.0
```

b) a configuração de NAT de R8, sabendo que todas as máquinas da rede inside têm o seu endereço mapeado para a interface outside deste router;

25%

```
interface e0
   ip address 192.168.15.1 255.255.255.0
   ip nat inside
interface e1
   ip address 193.139.15.1 255.255.255.0
   ip nat outside
ip nat inside source list 80 interface e1 overload
access-list 80 permit 192.168.15.0 0.0.0.255
```

c) a configuração de encaminhamento de R6;

25%

```
router rip
    version 2
    network 193.139.15.0
router ospf 100
    redistribute rip subnets
    network 193.138.51.0 0.0.0.255 area 2
    area 2 nssa
```

d) a configuração de OSPF e BGP de R0, sabendo que este router só deve anunciar para os outros sistemas autónomos as rotas com origem no próprio sistema autónomo.

30%

```
router ospf 100
      network 193.137.2.0 0.0.0.255 area 0
      network 193.137.3.0 0.0.0.255 area 0
router bgp 2000
      no synchronization
      bgp dampening
      no auto-summary
      redistribute ospf 100
      network 193.138.50.0 mask 255.255.255.0
      network 193.138.150.0 mask 255.255.255.0
      neighbor 193.138.50.2 remote-as 1000
      neighbor 193.138.50.2 filter-list 1 out
      neighbor 193.138.150.2 remote-as 3000
      neighbor 193.138.150.2 filter-list 1 out
      ip as-path access-list 1 permit ^$
```