Grupo I

1. O processo de self-healing em redes de núcleo é a capacidade da rede de detetar e corrigir automaticamente falhas, garantindo uma operação contínua.
2. O AS number identifica de forma única um sistema autónomo na Internet. É usado no BGP para estabelecer relações de vizinhança e encaminhar tráfego entre diferentes AS.
3. Policing aplica limites ao tráfego, ou seja, descarta pacotes que excedem a largura de banda permitida. Shaping suaviza o tráfego, fazendo o armazenamento de pacotes em filas para evitar perdas.
4. O RED não é frequentemente usado em redes comerciais, uma vez que é complexo de configurar e pode não ser eficiente em cenários de tráfego dinâmico.
5. A arquitetura spine-and-leaf é um design de rede datacenter onde switches leaf conectam servidores e switches spine interligam os leafs.
6. As FECs em MPLS agrupam pacotes que partilham o mesmo destino ou tratamento na rede. Quando associadas ao endereço MAC destino, permitem encaminhamento eficiente com base em informações de camada 2.
7. O DNS redirection em CDNs é usado para direcionar os utilizadores ao servidor mais próximo ou menos congestionado, com base na localização e condições da rede.
8. Não, o RTSP não controla os erros da transmissão. Ele é usado para gerir sessões de streaming. A correção de erros é tratada por protocolos de transporte como TCP ou UDP.
9. O MGCP/H.248 é um protocolo de controlo usado em VoIP para gerir gateways de media. Ele separa o controlo da sinalização, permitindo que um call agent configure, modifique e termine conexões nos gateways.
10. A transcodificação em VoIP é usada para converter entre diferentes codecs de áudio, permitindo compatibilidade entre dispositivos ou redes com capacidades distintas.
11. As probes RMON são usadas para monitorizar e analisar o desempenho da rede, capturando dados sobre tráfego, erros e estatísticas de utilização.

Grupo II

A. Em BGP, o atributo mais frequentemente preferido para definir preferências é o Local Preference. Este atributo é amplamente utilizado porque permite influenciar o encaminhamento dentro de AS, indicando qual rota deve ser preferida para saída. É propagado para todos os routers do AS, garantindo consistência no encaminhamento interno. Comparado a outros atributos como MED ou AS-Path, o Local Preference é mais eficaz em cenários internos, pois oferece maior controlo sobre as políticas de saída sem depender de configurações externas.
B. Ao escolher entre os modos downstream on-demand e downstream unsolicited para estabelecimento de LSPs, considera-se a eficiência e a flexibilidade. O modo on-demand é ideal para redes com requisitos dinâmicos, pois estabelece etiquetas apenas quando solicitadas, reduzindo o uso de recursos. Já o modo unsolicited é preferido em redes onde há tráfego previsível, pois distribui etiquetas

automaticamente, garantindo menor latência no encaminhamento. A decisão depende das necessidades de escalabilidade, simplicidade e tipo de tráfego da rede.

C. O modelo leaky bucket é preferido em certas implementações de QoS por oferecer um controlo rigoroso do fluxo de tráfego, enviando pacotes a uma taxa fixa, independentemente de variações de entrada. Este comportamento é ideal para cenários onde a regularidade do tráfego é essencial, como aplicações sensíveis a jitter. Em contraste, o token bucket permite ráfagas ao acumular tokens, o que pode causar variações de atraso. Assim, leaky bucket é mais simples e eficaz para tráfego constante.
D. O uso de BGP EVPN e VXLAN em conjunto não representa redundância, mas uma combinação de funcionalidades complementares. O VXLAN oferece uma solução para a expansão de redes de camada 2 sobre infraestruturas de camada 3, permitindo maior escalabilidade e isolamento através de VNIs. Já o BGP EVPN atua como o plano de controlo, distribuindo informações sobre MAC e IP de forma eficiente entre endpoints. Assim, o VXLAN é o plano de dados, enquanto o BGP EVPN organiza e otimiza a comunicação.
E. Desenvolver soluções de multimédia sem buffering é desafiador devido à necessidade de garantir uma reprodução contínua mesmo em condições de rede instáveis. No entanto, pode ser desejável em aplicações de tempo real, como chamadas VoIP ou videoconferências, onde a latência mínima é prioritária. Sem buffering, os dados são processados diretamente à medida que chegam, reduzindo atrasos, mas aumenta a probabilidade de interrupções em redes congestionadas. Este modelo é usado quando baixa latência supera a necessidade de estabilidade no fluxo.
F. Existem duas funções de transição principais para interligar redes telefónicas e redes IP devido às diferenças fundamentais entre os seus modelos. A Media Gateway converte os formatos de voz e sinalização analógica ou digital das redes telefónicas para pacotes IP, garantindo compatibilidade no transporte de áudio. Já o Signaling Gateway traduz protocolos de sinalização como SS7 para SIP ou H.323, permitindo o controlo das chamadas entre as redes. Estas funções são separadas para modularidade, facilitando escalabilidade e gestão.
G. Sim, o SNMP pode continuar a ser usado mesmo em sistemas que necessitem de CMIS, devido à sua simplicidade e baixo custo de implementação. Enquanto o CMIS/CMIP oferece capacidades avançadas, como modelos ricos de objetos e gestão transacional, o SNMP é leve e mais adequado para dispositivos com recursos limitados ou onde a complexidade de CMIS não é justificada. Em redes modernas, muitas vezes uma solução híbrida pode equilibrar simplicidade e funcionalidade, dependendo das necessidades específicas do sistema.

Grupo III

OA. Os serviços de interligação entre redes IP e redes telefónicas podem ser categorizados em funções de mediação e de transporte. Primeiramente, há o serviço de Media Gateway, que converte os formatos de voz analógica/digital em pacotes IP. Este serviço é essencial para suportar chamadas VoIP em redes legadas, como acontece com o Cisco Unified

Border Element, usado para integração de redes telefónicas tradicionais com plataformas de VoIP. Em segundo lugar, destacam-se os serviços de Signaling Gateway, que traduzem protocolos de sinalização como SS7, usado nas redes telefónicas, para protocolos como SIP, usados nas redes IP. Um exemplo comercial seria o Dialogic IMG Gateway, que suporta esta transição mantendo a interoperabilidade entre os dois mundos. Além disso, podem ser sugeridos serviços de Softswitch, que unem controlo de sinalização e media, gerindo chamadas entre redes IP e telefónicas. Um exemplo seria o Metaswitch, que oferece soluções integradas de VoIP e PSTN. Por fim, há serviços de Transcodificação, necessários para adaptar codecs de áudio entre os padrões telefónicos e os usados em IP, como acontece no Ribbon Communications Media Gateway, que permite interoperabilidade ao ajustar diferenças de compressão e qualidade de áudio. Estes serviços garantem uma integração eficiente e flexível entre tecnologias distintas.

OB. A escolha entre RSVP-TE e CR-LDP depende de vários fatores técnicos e de implementação. O RSVP-TE é mais adequado quando há necessidade de reservas explícitas de recursos, pois suporta sinalização stateful e possui extensões robustas para engenharia de tráfego. É ideal em redes onde a granularidade no controlo de fluxos é prioritária, como em ISPs que implementam MPLS para garantir QoS. Além disso, o RSVP-TE é mais amplamente adotado, suportado por diversos fabricantes e padronizado pelo IETF, o que facilita a interoperabilidade. Por outro lado, o CR-LDP oferece uma abordagem simplificada, com menor overhead de sinalização, utilizando sessões TCP persistentes para distribuir etiquetas. É mais eficiente em redes onde o foco está na escalabilidade e simplicidade, especialmente quando não há requisitos rigorosos para reservas de recursos. No entanto, o CR-LDP foi descontinuado pelo IETF, o que limita o suporte em equipamentos modernos. Assim, a escolha recai sobre o contexto da rede: RSVP-TE é preferido em implementações que exigem controlo detalhado de recursos e conformidade com padrões, enquanto o CR-LDP poderia ser usado em cenários menos exigentes onde simplicidade é uma prioridade, embora sua descontinuidade o torne menos viável atualmente.

OC. A relação entre a matriz de gestão TMN (Telecommunications Management Network) e o modelo FCAPS (Fault, Configuration, Accounting, Performance, Security) reside na complementaridade dos seus objetivos e estrutura. A TMN define uma arquitetura hierárquica para a gestão de redes de telecomunicações, com camadas de planeamento, operação e execução, organizando funções de gestão através de interfaces padronizadas. Já o modelo FCAPS fornece uma taxonomia funcional para classificar as atividades de gestão em cinco áreas principais: deteção e resolução de falhas (Fault), configuração de recursos (Configuration), contabilização (Accounting), monitorização de desempenho (Performance) e gestão de segurança (Security). A integração entre os dois modelos permite que a TMN adote o FCAPS como estrutura funcional para implementar tarefas específicas em cada camada da sua arquitetura. Por exemplo, na camada de gestão de rede da TMN, o modelo FCAPS pode ser aplicado para detetar falhas nos elementos de rede, configurar dispositivos remotamente e medir a performance geral. Além disso, enquanto o TMN define como os sistemas de gestão comunicam entre si, o FCAPS especifica o que precisa ser gerido, complementando o foco arquitetural da TMN com uma

visão funcional. Assim, os dois modelos operam em sinergia, combinando organização estrutural e categorização funcional para uma gestão eficiente.