**Grupo I**

**1. Quando um comutador Ethernet processa uma trama e o endereço IP de destino é desconhecido nas suas tabelas de encaminhamento, a trama é encaminhada para todas as interfaces, excepto a de origem.**

R: Falsa. Quando um comutador Ethernet processa uma trama e o endereço MAC…

**2. Para se explorar as capacidades de uma MIB privada é necessário que esta informação exista no manager e no agente residente no sistema que se pretende gerir.**

**R:** Verdadeiro. A MIB privada é feito pelo fabricante do dispositivo e contém funcionalidades específicas ao dispostivo. Para utilizar essas capacidades extra, é necessário que tanto o manager e o agente tenham essa MIB instalada.

**3. Um trap SNMP é gerado pelo manager sempre que é produzida uma alteração numa variável monitorizada no agente.**

**R:** Falso. pelo Agente.

**4. Na Análise de Requisitos está identificado o problema do “last-mile” como sendo a limitação da utilização da largura de banda disponível na infra- estrutura do Operador além da interface do sistema.**

**R:** Falso. last-foot.

**5. O MTBF é um parâmetro que é expresso em unidades de tempo e representa a probabilidade de avaria de um sistema/equipamento.**

**R:** Falso, representa o tempo médio entre avarias.

**6. Na Análise de Requisitos devem ser consideradas dois tipos de aplicações do ponto de vista da capacidade, as aplicações de tempo real e as que não são de tempo real.**

**R:** Falso. Nao é capacidade é delay. Nao sei se é necessário dividir as de nao tempo real em assíncronas e interativas.

**7. O OSPF é o protocolo de routing do tipo EGP mais utilizado na Internet devido à sua simplicidade, não suportar endereços de máscara variável, ter rápida convergência e ser um standard do IETF.**

**R:** Falso. IGP. Complexo e Suporta endereços de máscara variavel. ( na tabela nos slides diz que nao é simples)

**8. A disponibilidade é um parâmetro que tem um valor percentual e representa a probabilidade de avaria de um sistema/equipamento.**

**R:** Falso, representa a probabiblidade de um sistema/equipamento estar operacional.

**9.No protocolo SNMP são previstas quatro operações básicas: poll, set, getbulk e**

**trap.**

**R:** Falso. São três : get, set e trap.

**10. O BGP4 é um protocolo de routing do tipo EGP e pode ser usado para trocar**

**informação de routing entre routers dentro do mesmo Sistema Autónomo.**

**R:** Falso. Entre routers de diferentes AS’s.

**Grupo II**

**1- Apresente os protocolos de routing mais relevantes que conhece para a gestão das rotas de acesso a uma infra-estrutura de rede média e grande dimensão. Descreva o seu modo de operação (a colecção da informação de routing e a construção final da tabela de routing, etc.) e faça uma avaliação comparativa entre eles.**

**R:** Routing Interno - OSPF, EIGRP, IBGP, IGRP,

Routing Externo - BGP4

OSPF vs EIGRP vs IS-IS

OSPF - protocolo standard pelo IETF, pode ser utilizado por qualquer fabricante. É um protocolo do tipo link-state, sendo desta forma mais eficiente mas exigindo maior capacidade de processamento.

Os nós anunciam pela rede apenas os seus pacotes link-state (LSP) para informar os outros do seu estado. Com os LSP recebidos dos vizinhos, será então construído um modelo global de rede e a tabela de routing. Os melhores caminhos são calculados usando o algoritmo de Djsktra’s.

EIGRP - É um protocolo de routing do tipo distance-vector, sendo um melhoramento do IGRP: apenas envia partes da sua tabela de routing que outros nós não conhecem. em vez de a enviar por completo. Isto traz a vantagem de desocupar alguma largura de banda, sendo importante para redes de média ou grande dimensão. É propriedade da Cisco.

IS-IS - protocolo standard pelo OSI, semelhante ao OSPF mas desenvolvido para atuar sobre IP, visto que é um protocolo OSI da camada 3.

Conclusão:

-> Os três protocolos têm tempo de convergência baixo ~1segundo

-> São complexos

-> Métricas:

- OSPF - Custo = Ref bw / interface bw

- EIGRP - com base no atraso e largura de banda

- IS-IS - peso de 10 a cada ligação???

-> OSPF e IS-IS dividem a rede em áreas, sendo que o OSPF necessita que as áreas sejam adjacentes á área 0

-> OSPF suporta mais funcionalidades, IS-IS é mais escalável e para os mesmos recursos suporta mais routers, no entanto é mais complexo.

**2- Caracterize o protocolo SNMP, fazendo referência à evolução das várias versões. Descreva sumariamente as alterações importantes introduzidas com o SNMPv3.**

**R:** SNMP é usado para gerir dispositivos na rede, constituído por agente-gestor, com várias informações sobre todos os dispositivos.

A primeira versão permite ler,escrever e receber avisos por parte dos agentes sobre eventos. Tem uma community string em texto, que pode ser facilmente descoberta. É pouco eficiente no desempenho.

A segunda versão tem melhorias no desempenho, permite outros protocolos como OSI e IPX, têm uma árvore maior, uma MIB mais completa com mais códigos de erro.

As alterações importantes na versão 3 são o facto de a community string e authentication string serem encriptadas e o protocolo estar dividido em subsistemas, sendo um deles responsável pela segurança. É uma versão mais pesada, que necessita de dispositivos com melhor desempenho. É feita a verificação da autenticação ( através do uso de uma string de autenticação) e a verificação da integridade dos dados (não permite alterar a ordem nem o conteúdo dos dados).

**3- Caracterize o problema da segurança num sistema de gestão baseado no SNMP. Indique quais as possíveis ameaças à segurança, em que partes do modelo de gestão podem existir e quais as soluções recomendadas.**

**R:** As versões 1 e 2 do protocolo SNMP estão sujeitas a packet sniffing da community string, pois esta não circula encriptada, sendo enviada em texto simples.

No entanto, todas as versões estão sujeitas a brute-force para descobrir a community string e string de autenticação.

* Ameaças principais:
  + Disfarce de autenticação da origem - o intruso assume a identidade do remetente.
  + Alteração da informação/ integridade dos dados.
* Ameaças secundárias:
  + Alteração da sequência das mensagens
  + Exposição de confidencialidade dos dados
* Outras ameaças:
  + Denial of Service (DDOS)
  + Análise de Pacotes

**4 - Explique o que é uma MIB RMON, qual a sua utilidade e como é que esta poderá ser usada para a gestão de sistemas e serviços.**

**R:** Uma MIB RMON (Remote Monitoring) permite a troca de dados ou monitorização da rede entre vários sistemas. Funciona em cliente/servidor onde os equipamentos monitorizados, sondas RMON, têm instalado um software que coleciona informação e analisa pacotes. Estas sondas atuam como servidores e as aplicações de gestão como clientes. Tanto a configuração dos agentes como

**5 - Responda às seguintes questões sobre Planeamento, apresentando uma breve justificação:**

1. **Na análise de requisitos para o planeamento da rede há diferentes tipos de requisitos? Quais e como os organiza?**

**R:** Para a análise de requisitos para o planeamento da rede existem os seguintes requisitos:

* **Requisitos de utilizadores** - prontidão, interatividade, funcionalidade, segurança, fiabilidade, crescimento futuro, custo.
* **Requisitos de aplicações** - podem ser do tipo real-time, rate-critical ou mission critical -
* **Requisitos dos equipamentos/dispositivos** - tipo de equipamento, localização e performance
* **Requisitos da rede** - Gestão de redes, objetivos técnicos como a disponibilidade, a performance

1. **Qual a importância da localização dos equipamentos na análise de requisitos?**

**R:** A loclização dos equipamentos na análise de requisitos é importante para estabelecer relações entre aplicações, utilizadores e dispositivos. É especialmente importante quando temos elementos da rede colocados remotamente, que exigem um planeamento antecipada para garantir comunicação remota sem problemas.

1. **Que tipo de aplicações distingue na análise de requisitos relativamente ao atraso? Caracterize-as?**

**R:** Tempo real (teleconferência)

Não tempo real - interativas (bulk - telnet ; bursts - ftp)

- assíncronas - email

1. **Qual a diferença de avaliação dos problemas “last foot” e “last mile”?**

**R:** O problema last-foot descreve a dificuldade de fazer entregar toda a capacidade de serviço desde o equipamento até à interface do sistemas do utilizador. Pode resultar do facto do hardware disponível já estar desatualizado, o que faz com que a performance da ligação não seja a melhor possível.

O problema last-mile descreve a dificuldade de levar toda a qualidade de serviço desde a infraestrutura do operador até à propriedade do cliente.

1. **Quais as implicações da introdução de procedimentos de gestão da rede a considerar no projecto lógico e, posteriormente, na exploração da rede?**

**R:**

**Grupo III**

**1.**

email- client-server

web : client -server

voip: cliente-server no setup e terminaçao

peer-to-peer no flow da chamada

sap: client-server

**2.** GW1 - ISP2

GW1- ISP1

GW2 - ISP1

GW3 - ISP1

todos LAN/WAN.

**3.**

**Email**

96+480 + (120 + 20 ) \* 2 = 856 No enunciado diz que cada utilizador tem um terminal VoIP mas nao ha suficientes para todos os utilizadores e agora ? usamos o numero de utilizadores ou o numero de terminais voip ?

**SEDE- ISP1**

Entrar na sede (incoming) : 25 M \* 8 \* 0,7\*856 / 86400 =1,4 Mb/s

Sair da sede (outgoing) : 10M \* 8 \* 856 \* 0,4 / 28800 = 0,95 Mb/s

**SEDE - FILIAL**

sair da sede/entrar na filial : 25 M \* 8 \* 140 / 28800 = 0,972Mb/s

entrar na sede/sair da filial : 10M \* 8 \* 140 / 28800 = 0,389Mb/s

**WEB.**

SEDE - ISP

entrar na sede : 40 M \* 8 \* 856 / 28800 = 9,51Mb/s

SEDE - filial

entrar na filial : 50M \* 8 \* 140 / 28800 = 1,9 Mb/s

**VOIP:**

**300 + 96 + (20+60) \*2 = 556**

**SEDE - ISP**

a entrar na sede : 2M \* 8 \* 556 / 28800 = 0,309Mb/s

a sair da sede : 0,309Mb/s

**SEDE - FILIAL**

Entrar e sair :2M \* 8 \* 80 / 28800 = 0,044Mb/s

**SAP:**

0,1 \* 140 \* 15kbytes \* 8 \*20 /28800 = 1,2kb/s

d)

Entrar na sede : 1,4 + 0,389 \*2 + 9,51 + 0,309 + 0,044\*2 = 12,085 Mb/s

Sair da sede : 0,95 + 0,972 \* 2 + 1,9 + 0,309 + 0,044 \* 2 = 5,191 Mb/s