

Nome do estudante: .....

- Escreva o nome no cabeçalho de todas as folhas de exame que entregar;
- Apresente as respostas na sua folha de exame segundo a ordem correspondente do enunciado;
- Leia atentamente o enunciado e procure responder de uma forma clara e sucinta às questões que se lhe colocam.

Grupo I – (30 min) Indique para cada uma das afirmações se a considera verdadeira ou falsa; reescreva completamente as afirmações falsas com as correcções necessárias para serem verdadeiras. A correcção de uma afirmação falsa recorrendo apenas à negação desta não é cotada. Geralmente, para construir uma afirmação verdadeira basta trocar ou acrescentar de uma a três palavras na afirmação falsa.

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.

---

---

---

- ?  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.

---

---

---

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

---

---

---

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

---

---

---

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.  
*atraso*

---

---

---

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

---

---

---

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

---

---

---

Prova sem consulta. Duração: 2h00min

Exemplo

9. No protocolo SNMP são previstas quatro<sup>3</sup> operações básicas: poll, set, getbulk 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. de diferentes

---

---

---

Prova sem consulta. Duração: 2h00min

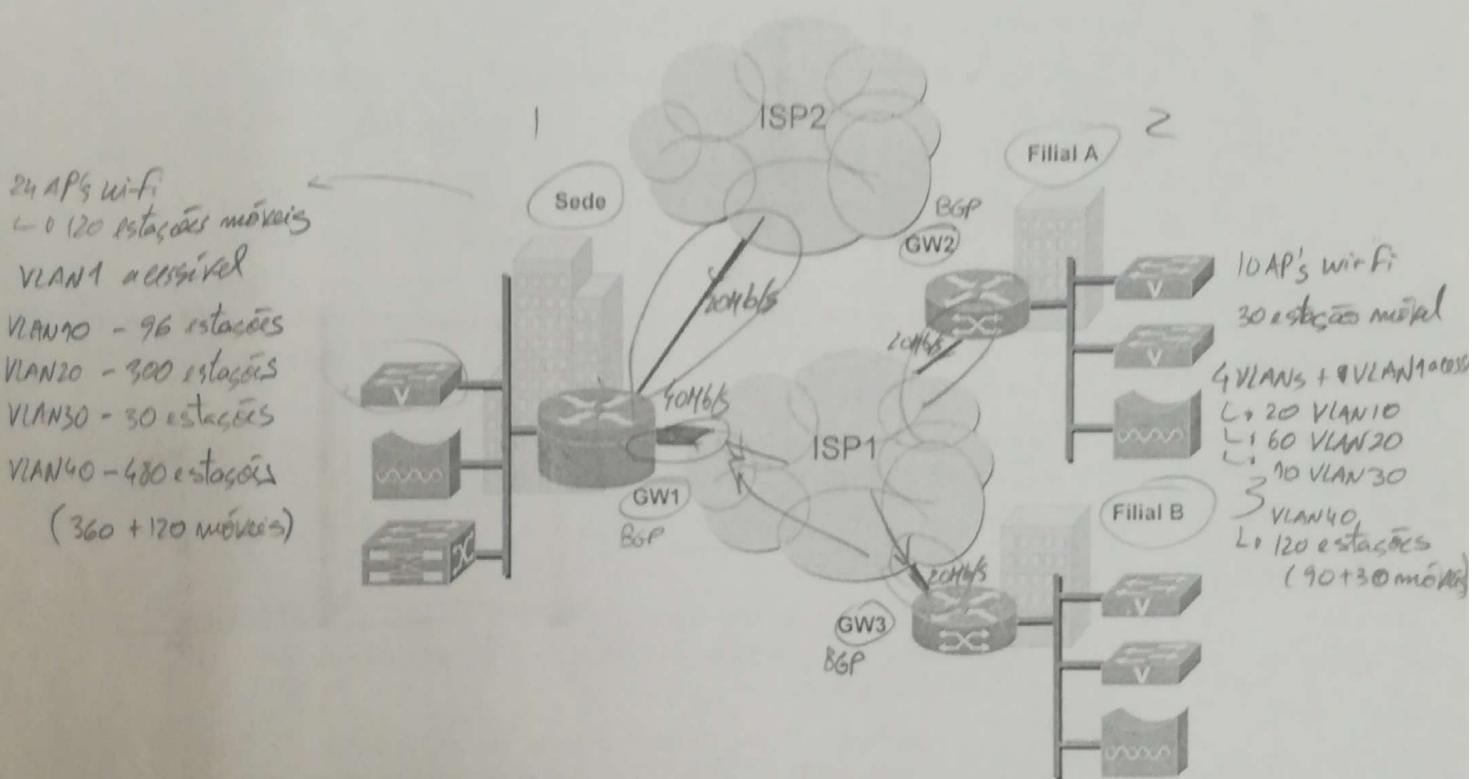
Exemplo

Grupo II – (45 min) Responda objectiva e sucintamente às seguintes questões, justificando todas as respostas:

*OSPF, BGP  
pode ser RIP? EIGRP??*

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. *link-state : OSPF, EIGRP, IS-IS?*
2. Caracterize o protocolo SNMP, fazendo referência à evolução das várias versões. Descreva sumariamente as alterações importantes introduzidas com o SNMPv3.
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.
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.
5. Responda às seguintes questões sobre Planeamento, apresentando uma breve justificação:
  - a) Na análise de requisitos para o planeamento da rede há diferentes tipos de requisitos? Quais e como os organiza?
  - b) Qual a importância da localização dos equipamentos na análise de requisitos?
  - c) Que tipo de aplicações distingue na análise de requisitos relativamente ao atraso? Caracterize-as?
  - d) Qual a diferença de avaliação dos problemas "last foot" e "last mile"?
  - e) Quais as implicações da introdução de procedimentos de gestão da rede a considerar no projecto lógico e, posteriormente, na exploração da rede?

**Grupo III – (45 min)** A empresa QQCOISA Lda tem as instalações, sede e filiais, localizadas em três cidades distintas. O edifício sede e as filiais comunicam entre si em IP com ligações directas à Internet em Ethernet a 40 Mb/s e 20 Mb/s, respectivamente. Adicionalmente tem no edifício sede um segundo acesso à Internet através de outro ISP. As características principais das infra-estruturas de rede da empresa são abaixo apresentadas, tendo em consideração o número máximo de estações previsto para cada rede local:



- Todos os serviços da rede são suportados na pilha de protocolos TCP/IP.
- Todos os routers GW1, GW2 e GW3 dialogam entre si em BGP e estão dentro do mesmo Sistema Autónomo (AS).
- Em cada edifício das filiais estão previstos:
  - 10 APs Wi-Fi para dar acesso em qualquer ponto do edifício a 30 estações móveis;
  - 4 VLANs (para além da VLAN1 que se pretende acessível) com 20 estações na VLAN10 para os serviços administrativos e gestão, 60 estações na VLAN20 para os terminais VoIP, 10 estações na VLAN30 para os servidores locais e 120 estações (já incluídas as estações móveis) na VLAN40 para os utilizadores comuns da rede.

- No edifício sede estão previstos:
  - 24 APs Wi-Fi para dar acesso em qualquer ponto do edifício a 120 estações móveis;
  - 4 VLANs (para além da VLAN1 que se pretende acessível) com 96 estações na VLAN10 para os serviços administrativos e gestão, 300 estações na VLAN20 para os terminais VoIP, 30 estações na VLAN30 para os servidores de toda a empresa e 480 estações (já incluídas as estações móveis) na VLAN40 para os utilizadores comuns da rede.

Considerando o número de postos de trabalho indicado e assumindo que cada utilizador tem acesso a um posto de trabalho e um terminal VoIP, considere os seguintes padrões de tráfego:

- E-mail – cada utilizador envia em média 10 Mbyte por dia e recebe 25 Mbyte, durante as 8 horas de trabalho. O tráfego recebido tem o seguinte padrão: cerca de 70% tem origem no exterior e o restante é interno da empresa. O tráfego enviado tem o seguinte padrão: cerca de 60% destina-se a endereços da própria empresa, sendo os restantes 40% para destinatários externos;
- Acesso Web – cada utilizador acede em média a 10 Mbyte de conteúdos da empresa e 40 Mbyte de conteúdos externos;
- VoIP – em média cada utilizador consome no total 2 Mbyte de tráfego de entrada e de saída;
- SAP – só 10% dos utilizadores das filiais e 20% do edifício sede usam o SAP; as transacções médias de dados são de 15 kbyte. Cada utilizador faz uma média de 20 transacções diárias;
- Backup – é transferido diariamente, a partir das 00:00 até às 07:00, dos servidores localizados no edifício sede para os servidores alojados nas instalações de um *Service Provider*, uma cópia de segurança dos documentos gerados localmente, com o volume total médio de 5 Gbyte.

1. Qual o modelo de fluxos que caracteriza cada um destes fluxos na rede?
2. Quais são as fronteiras importantes dos fluxos da rede da empresa?
3. Quantifique com valores aproximados os fluxos de E-mail, acesso web, VoIP e SAP entre edifícios. (*VoIP manda email??*)
4. Discuta o débito disponibilizado nos acessos à Internet no edifício sede, tendo em consideração os valores obtidos na pergunta anterior.

*Cada utilizador usa VoIP e serviços de gestão ...*

**FIM**

*⑦ Na análise dos débitos interessam os valores de tráfego trocado c/o exterior...  
os dados internos não entram nas contas, caso seja entre edifícios ??*

Faculdade de Engenharia da Universidade do Porto

Mestrado Integrado em Engenharia Electrotécnica e de Computadores

Unidade Curricular de PGRE

Exemplo de Exame, duração: 2h00min

- Escreva o nome e o número no cabeçalho de todas as folhas de exame que entregar;
- Apresente as respostas na sua folha de exame segundo a ordem correspondente do enunciado;
- Leia atentamente o enunciado e procure responder de uma forma clara e sucinta às questões que se lhe colocam.

Grupo I (40min) *questões*

Responda às seguintes questões, apresentando uma breve justificação:

1. Na análise de requisitos, no planeamento de uma rede, é recomendado considerar os requisitos do utilizador. Diga quais são e faça uma breve descrição de cada um.
2. Quais os requisitos específicos da rede que considera no planeamento desta? Caracterize-os.
3. E quais os requisitos que deverá considerar para o planeamento da componente de gestão?
4. O que entende por SLA e qual a relevância que lhe reconhece?
5. Qual a importância da localização dos equipamentos na análise de requisitos?
6. Diga o que entende por um serviço de acesso à Internet com 99,50% de disponibilidade.
7. O que indica o valor de MTTR? Qual a sua relevância?
8. Quais os factores que considera na avaliação do desempenho da uma rede?
9. Na análise de fluxos, que tipo de fluxos é que distingue e quais as implicações da previsão de cada um?
10. Indique e descreva quais os modelos de fluxos que considera.

## Grupo II (40min)

Fluxos

Uma empresa tem instalações localizadas em duas cidades. Em cada cidade existe uma rede local e estão interligadas por uma VPN/IP. Na cidade A, onde está o edifício sede, existem 120 utilizadores e na cidade B 20. A saída de todo o tráfego da empresa para a Internet é feito exclusivamente pela cidade A. Todo o tráfego de E-mail da empresa passa obrigatoriamente pelos servidores localizados em A, havendo na cidade B um servidor de E-mail para a distribuição local. Os servidores das restantes aplicações (Web, SAP e backup) estão residentes na cidade A.

- E-mail – cada utilizador envia em média 10MB por dia e recebe 25MB, durante as 8 horas de trabalho. O tráfego recebido tem o seguinte padrão: cerca de 70% tem origem no exterior e o restante é interno da empresa. O tráfego enviado tem o seguinte padrão: cerca de 60% destina-se a endereços da própria empresa, sendo os restantes 40% para contactos exteriores; C-S
- Acesso Web – cada utilizador em média acede a 10MB de conteúdos da empresa e 30MB de conteúdos externos; C-S
- SAP – só 10% dos utilizadores em cada cidade usam o SAP e as transacções médias de dados são de 15KB. Cada utilizador faz uma média de 30 transacções diárias; C-S
- Backup – é transferido diariamente, a partir das 00:30 até às 06:30, da cidade B para a cidade A, uma cópia de segurança dos documentos gerados localmente, com o volume total médio de 3 GB. C-S

1. Caracterize os fluxos desta rede.
- ✓ 2. Quais são as fronteiras importantes dos fluxos da rede da empresa?
3. Quantifique os fluxos de E-mail, acesso web e SAP entre cidades.
4. Calcule o débito mínimo recomendado para o acesso de cada cidade, assim como o débito para a Internet na cidade A.

### Grupo III (20min)

V/F

Leia com atenção cada uma das afirmações abaixo apresentadas e indique para cada uma delas se a considera verdadeira ou falsa. Reescreva completamente as afirmações que considera falsas fazendo as correções necessárias para as tornar verdadeiras (A correcção de uma afirmação falsa recorrendo apenas à negação desta não é cotada).

1. O SNMP é um conjunto de standards para a gestão exclusiva de redes locais, que inclui um ou mais protocolos.
2. Um trap SNMP é gerado pelo manager sempre que é produzida uma alteração numa variável monitorizada no agente.
3. O SNMP ~~y~~<sup>1</sup> enquadra-se no modelo de camadas TCP/IP, sobre a camada de transporte TCP.
4. 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.
5. Uma das grandes vantagens do SNMP é permitir fazer a gestão remota de equipamento de uma rede, garantindo a segurança das comunicações entre o sistema de gestão e os agentes residentes nos equipamentos.
6. O OID é ~~um dos vários~~ identificadores possíveis de um objecto em particular da árvore de gestão da Internet.
7. Uma sonda RMON permite ao gestor estender as funções da gestão ao coleccionar os traps ocorridos na parte da rede em que está inserida.
8. No Subsistema de Segurança do modelo SNMPv3 é o que é realizada a codificação e decifragem das mensagens privadas do protocolo.

### Grupo IV (20min) *Questões*

Responda sucintamente às seguintes questões

1. Apresente quais são as áreas funcionais do modelo OSI de gestão de redes e explique cada uma delas.
2. Caracterize o problema da segurança num sistema de gestão de uma rede baseado no SNMP. Indique quais as possíveis ameaças à segurança, em que partes do modelo de gestão podem existir e quais as soluções recomendadas.
3. Explique o que é uma MIB privada de um fabricante, qual a sua necessidade e como é que esta poderá ser usada para a gestão do respectivo sistema na rede.

FIM

Nome do estudante: .....

- Escreva o nome no cabeçalho de todas as folhas de exame que entregar;
- Apresente as respostas na sua folha de exame segundo a ordem correspondente do enunciado;
- Leia atentamente o enunciado e procure responder de uma forma clara e sucinta às questões que se lhe colocam.

**Grupo I – (25%)** Indique para cada uma das afirmações se a considera verdadeira ou falsa; reescreva completamente as afirmações falsas com as correções necessárias para serem verdadeiras. A correção de uma afirmação falsa recorrendo apenas à negação desta não é cotada. Geralmente, para construir uma afirmação verdadeira basta trocar ou acrescentar de uma a três palavras na afirmação falsa.

1. Quando um router Ethernet processa um pacote e o endereço MAC de destino é desconhecido nas suas tabelas de encaminhamento, o pacote é encaminhado para todas as interfaces, exceto a de origem.

*switch*

*MAC*

✓

\_\_\_\_\_

2. Na comunicação entre duas estações localizadas em LANs distintas, um pacote transmitido pode ser fragmentado apenas uma vez e deverá ser reconstruído pelo último router que serve a LAN da estação de destino.

\_\_\_\_\_

✓

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

*agente*

\_\_\_\_\_

Prova sem consulta. Duração: 2h00min

Exame de Recurso



4. O SNMPv1 é uma solução de gestão de redes suportada nos protocolos de transporte TCP.

---

---

---



5. 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. *atraso*

---

---

---



6. Na Análise de fluxos, um fluxo *peer-to-peer* é caracterizado por uma hierarquia e uma direccionalidade. *cliente-servidor*

---

---

---



7. O Telnet é uma aplicação que do ponto de vista dos requisitos da capacidade pode ser classificada como tempo real. *do atraso*

---

---

---



8. Um endereço <sup>IPv4</sup> [IPv5] de uma rede com uma máscara de 22 bits a "1", permite endereçar no máximo 510 estações ativas na rede. 2048

---

---

---

$$(2^{10}) =$$

$$2^5 = 32 / 6 - 64 / 7 - 128 / 8 - 512 / 9 - 1024 / 10 - 2048$$

Prova sem consulta. Duração: 2h00min

Exame de Recurso

- Questões*
- Grupo II – (35%) Responda objetiva e sucintamente às seguintes questões, justificando todas as respostas:
1. Apresente as soluções mais relevantes que conhece, do ponto de vista do routing, para a gestão das rotas de acesso a uma infraestrutura de rede de média e grande dimensão. Descreva o seu modo de operação (a coleção da informação de routing e a construção final da tabela de routing, etc.) e faça uma avaliação comparativa entre elas. OSPF, BGP
  2. Apresente as áreas funcionais do modelo OSI de gestão de redes, descreva os procedimentos e objetivos para cada uma delas
  3. Caracterize o protocolo SNMPv3, fazendo referência às alterações importantes introduzidas nesta versão.
  4. Explique o que é uma MIB privada, quais as funcionalidades disponibilizadas e vantagens na sua utilização.
  5. Responda às seguintes questões sobre Planeamento, apresentando uma breve justificação:
    - a) O que entende por SLA e qual a relevância que lhe reconhece?
    - b) Qual a diferença de avaliação dos problemas "last foot" e "last mile"?
    - c) Comente quanto à disponibilidade um serviço de acesso à Internet com 99,50% comparativamente a outro com 95%.
    - d) Que tipo de aplicações distingue na análise de requisitos relativamente ao atraso? Caracterize-as.

Prova sem consulta. Duração: 2h00min

Exame de Recurso

9. O OSPF é o protocolo de routing do tipo IGP mais utilizado na Internet devido à sua complexidade, suportar endereços não alinhados à classe, ter rápida convergência e ser uma norma do IETF.

IETF

---

---

---

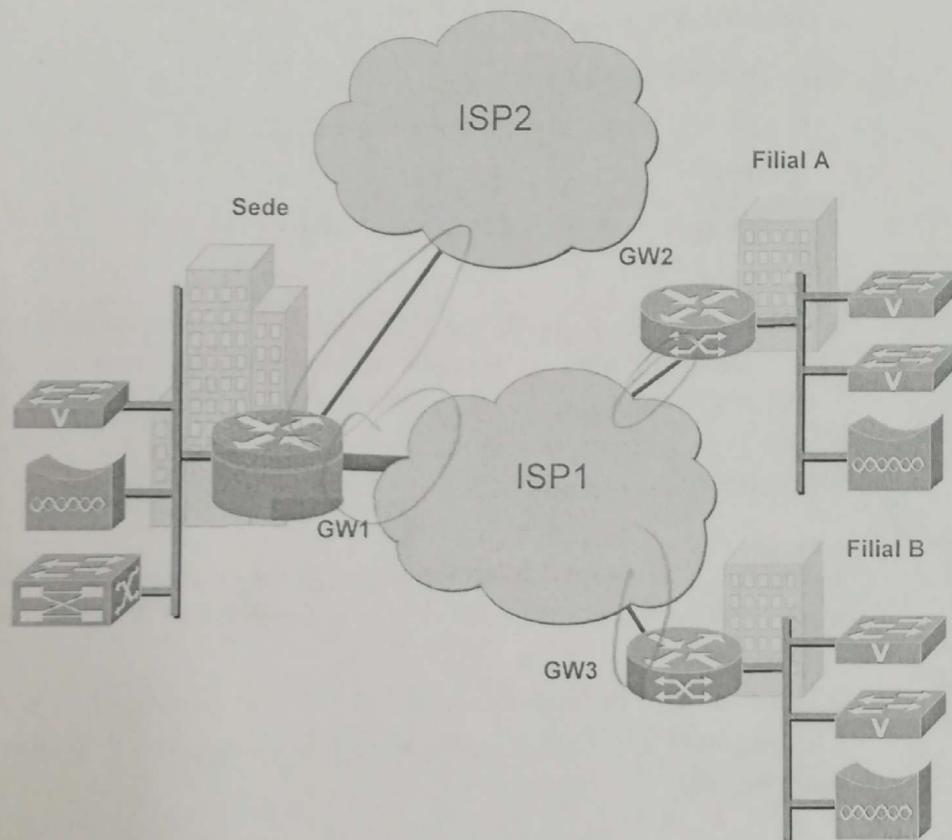
10. O BGP4 é um protocolo de routing exterior do tipo (distance vector)<sup>path</sup> e pode ser usado como um IGP para trocar informação de routing entre routers dentro do mesmo Sistema Autónomo.

---

---

---

**Grupo III – (40%)** A empresa QQCOISA Lda. tem as instalações, sede e filiais, localizadas em três cidades distintas. O edifício sede e as filiais comunicam entre si em IP com ligações diretas à Internet em Ethernet a 40 Mb/s e 20 Mb/s, respetivamente. Adicionalmente tem no edifício sede um segundo acesso à Internet através de outro ISP, reservado para o serviço de *Disaster Recovery*. As características principais das infraestruturas de rede da empresa são abaixo apresentadas, tendo em consideração o número máximo de estações previsto para cada rede local:



- Todos os serviços da rede são suportados na pilha de protocolos TCP/IP.
- Todos os routers GW1, GW2 e GW3 dialogam entre si em BGP e estão dentro do mesmo Sistema Autónomo (AS).
- Os circuitos de acesso ao ISP1 têm os endereços 84.155.41.65/30, 84.155.41.129/30 e 84.155.41.193/30 para os routers GW1, GW2 e GW3, respetivamente.
- O circuito de acesso ao ISP2 usa a rede de interligação 195.23.200.160/30, em que o endereço mais baixo é do router do ISP2.
- Em cada edifício das filiais estão previstos:

Prova sem consulta. Duração: 2h00min

Exame de Recurso

- ✓ - 10 APs Wi-Fi para dar acesso em qualquer ponto do edifício a 30 estações móveis;
- ✓ - 4 Ethernet switches a 10/100 Mb/s, com 48 portas RJ45 e suporte de "Inline Power";
- ✓ - 4 VLANs (para além da VLAN1 que se pretende acessível) com 20 estações na VLAN10 para os serviços administrativos e gestão, 60 estações na VLAN20 para os terminais VoIP, 10 estações na VLAN30 para os servidores locais e 120 estações (já incluídas as estações móveis) na VLAN40 para os utilizadores comuns da rede.
- No edifício sede estão previstos:
    - 24 APs Wi-Fi para dar acesso em qualquer ponto do edifício a 120 estações móveis;
    - 16 Ethernet switches a 10/100/1000 Mb/s, com 48 portas RJ45 e suporte de "Inline Power";
    - 4 VLANs (para além da VLAN1 que se pretende acessível) com 96 estações na VLAN10 para os serviços administrativos e gestão, 300 estações na VLAN20 para os terminais VoIP, 30 estações na VLAN30 para os servidores de toda a empresa e 480 estações (já incluídas as estações móveis) na VLAN40 para os utilizadores comuns da rede.

*Endereçamento*

✓ Para resolver o problema de endereçamento da empresa QQCOISA Lda foi-lhe atribuído o bloco de endereços 200.16.124.0/22 e 200.16.128.0/22.

- ✓ 1. Qual o número mínimo de redes que utilizava para resolver o endereçamento da empresa? Explique porquê, indicando o respetivo tamanho dos blocos de endereços.
- ✓ 2. Assumindo a atribuição de endereços que fez na pergunta anterior, apresente os vários endereços de identificação da rede, de broadcast e as respetivas máscaras, para cada uma delas.
- fluxos* 3. Considerando o número de postos de trabalho indicado e assumindo que cada utilizador tem acesso a um posto de trabalho e um terminal VoIP, sendo o horário de trabalho das 9:00 até as 18:00, considere os seguintes padrões de tráfego:
  - E-mail – cada utilizador envia em média 20 Mbyte por dia e recebe 80 Mbyte. Os servidores do serviço de E-mail estão alojados no edifício sede. O tráfego recebido tem o seguinte padrão: cerca de 70% tem origem no exterior e o restante é interno à empresa. O tráfego enviado tem o

seguinte padrão: cerca de 20% destina-se a endereços internos à empresa, sendo os restantes 80% para destinatários externos;

- ✓ • Acesso Web – cada utilizador acede em média a 30 Mbyte de conteúdos da empresa e 120 Mbyte de conteúdos externos, cada edifício tem um proxy server com acesso direto à Internet;
  - ✓ • VoIP – em média cada utilizador consome no total 4 Mbyte de tráfego de entrada e de saída, sendo 80% para o exterior;
  - ✓ • SAP – só 10% dos utilizadores das filiais e 20% do edifício sede usam o SAP; as transações médias de dados são de 15 kbyte. Cada utilizador faz uma média de 20 transações diárias;
  - ✓ • Backup – é transferido diariamente, a partir das 00:30 até às 06:30, dos servidores localizados no edifício sede para os servidores alojados nas instalações de um *Service Provider*, uma cópia de segurança dos documentos gerados localmente, com o volume total médio de 3 Gbyte.
- ✓ a) Qual o modelo de fluxos que caracteriza cada um destes fluxos na rede?
- ✓ b) Quais são as fronteiras importantes dos fluxos da rede da empresa?
- ✓ c) Quantifique com valores aproximados os fluxos de E-mail, acesso web e SAP em todos os edifícios.
- ✓ d) Discuta o débito disponibilizado nos acessos à Internet nos vários edifícios, tendo em consideração os valores obtidos na resposta à alínea anterior.

FIM

Prova sem consulta. Duração: 2h00min

Nome do estudante: .....

- Escreva o nome no cabeçalho de todas as folhas de exame que entregar;
- Apresente as respostas na sua folha de exame segundo a ordem correspondente do enunciado;
- Leia atentamente o enunciado e procure responder de uma forma clara e sucinta às questões que se lhe colocam.

**Grupo I – (25%)** Indique para cada uma das afirmações se a considera verdadeira ou falsa; reescreva completamente as afirmações falsas com as correções necessárias para serem verdadeiras. A correção de uma afirmação falsa recorrendo apenas à negação desta não é cotada. Geralmente, para construir uma afirmação verdadeira basta trocar ou acrescentar de uma a três palavras na afirmação falsa.

1. Na comunicação TCP/IP entre duas estações localizadas em redes diferentes e interligadas por um router, o IP endereço MAC de destino do pacote enviado pela estação de origem é o do router responsável pela interligação.

*do estação destino*

---

---

2. Na comunicação entre duas estações localizadas em LANs distintas, uma trama transmitida pode ser fragmentada várias vezes e deverá ser reconstruída pelo último router que serve a LAN da estação de destino.
- 
- 

??

3. Uma das grandes vantagens do SNMP é permitir fazer a gestão remota de equipamento de uma rede, garantindo a segurança das comunicações entre o sistema de gestão e os agentes residentes nos equipamentos.
- SNMPv3*
- 
-

Prova sem consulta. Duração: 2h00min

4. O SNMP é uma solução de gestão de redes locais suportada nos protocolos de transporte ~~TCP~~ e UDP.
- 
- 
- 
5. Na Análise de Requisitos devem ser consideradas dois tipos de aplicações do ponto de vista da ~~atraso~~ <sup>atraso</sup> capacidade, as aplicações ~~interativas~~ <sup>temporal</sup> e as ~~assíncronas~~ <sup>não tempo real</sup>.
- 
- 
- 
6. O ~~RIP~~, o BGP, o ~~OSPF~~ e o ~~HELLO~~, são protocolos de routing exterior que suportam a notação CIDR e permitem divulgar redes com máscara variável (VLSM).
- 
- 
- 
7. O OSPF é o protocolo de routing do tipo ~~EIGP~~ <sup>IGP</sup> mais utilizado na Internet devido à sua simplicidade, ~~não~~ suportar endereços de máscara variável, ter rápida convergência e ser uma norma do IETF.
- 
- 
- 
8. O MTTR é um parâmetro que tem um valor que expressa um intervalo de tempo e representa a ~~probabilidade de avaria de um sistema/equipamento~~ <sup>voltar a estar ativo</sup> o tempo médio de espera até o
- 
- 
-

Prova sem consulta. Duração: 2h00min

9. No modelo de gestão baseado no protocolo SNMP estão previstas três entidades fundamentais: o gestor, o agente e o protocolo de gestão. *e a informação do gestor*
- 
- 

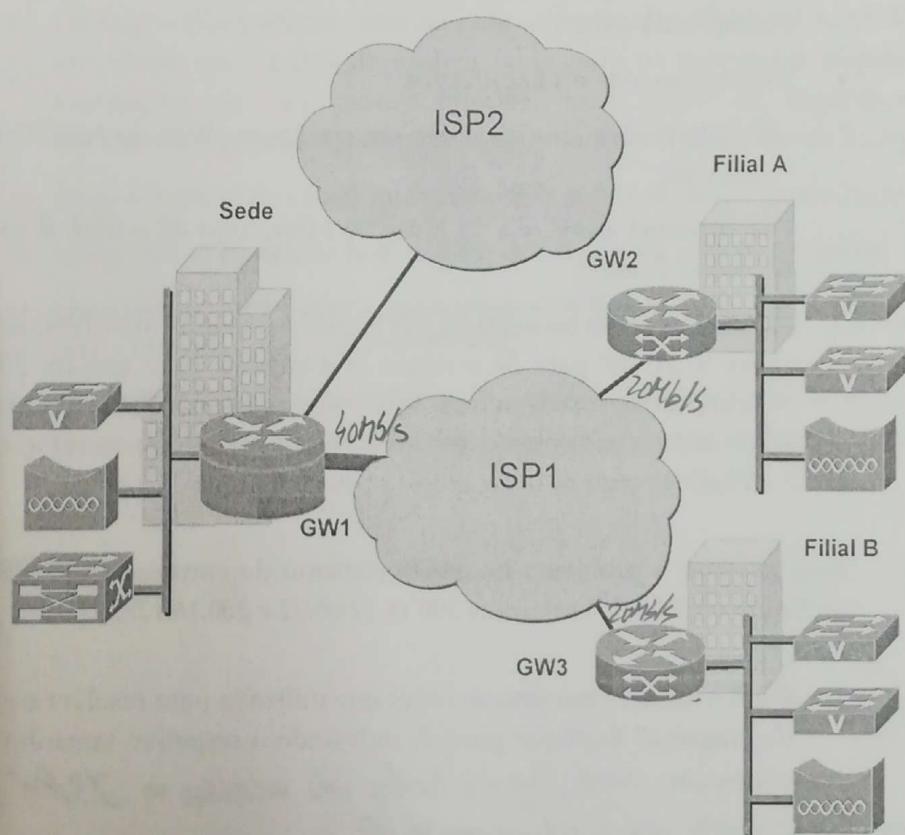
10. O OSPF é um protocolo de routing interior do tipo link-state e pode ser usado para trocar informação de routing entre routers dentro do mesmo Sistema Autónomo.
- 
-

Prova sem consulta. Duração: 2h00min

**Grupo II –** (35%) Responda objetiva e sucintamente às seguintes questões, justificando todas as respostas:

- ✓ 1. Apresente as soluções mais relevantes que conhece, do ponto de vista do routing, para a gestão das rotas de acesso a uma infraestrutura de rede de pequena e média dimensão. Descreva o seu modo de operação (a coleção da informação de routing e a construção final da tabela de routing, etc.) e faça uma avaliação comparativa entre elas. RIP, IGRP, OSPF
2. Apresente as áreas funcionais do modelo OSI de gestão de redes, descreva os procedimentos e objetivos para cada uma delas falhas / contabilização / configurações / desempenho / segurança
- ✓ 3. Caracterize o problema da segurança num sistema de gestão baseado no protocolo SNMP. Indique quais as ameaças à segurança e as soluções previstas no modelo do protocolo.
- ✓ 4. Explique o que é uma MIB RMON, quais as funcionalidades disponibilizadas e vantagens na sua utilização.
5. Responda às seguintes questões sobre Planeamento, apresentando uma breve justificação:
- O que entende por SLA e qual a relevância que lhe reconhece?
  - Qual a importância da localização dos equipamentos na análise de requisitos?
  - Diga o que entende por um serviço de acesso à Internet com 99,50% de disponibilidade. l, tempo s/ avarias
  - O que indica o valor do MTBF? Qual a sua relevância?  
mean time before failure

**Grupo III – (40%)** A empresa QQCOISA Lda. tem as instalações, sede e filiais, localizadas em três cidades distintas. O edifício sede e as filiais comunicam entre si em IP com ligações diretas à Internet em Ethernet a 40 Mb/s e 20 Mb/s, respetivamente. Adicionalmente tem no edifício sede um segundo acesso à Internet através de outro ISP, reservado para o serviço de *Disaster Recovery*. As características principais das infraestruturas de rede da empresa são abaixo apresentadas, tendo em consideração o número máximo de estações previsto para cada rede local:



- Todos os serviços da rede são suportados na pilha de protocolos TCP/IP.
- Todos os routers GW1, GW2 e GW3 dialogam entre si em BGP e estão dentro do mesmo Sistema Autónomo (AS).
- Os circuitos de acesso ao ISP1 têm os endereços 84.155.41.65/30, 84.155.41.129/30 e 84.155.41.193/30 para os routers GW1, GW2 e GW3, respetivamente.
- O circuito de acesso ao ISP2 usa a rede de interligação 195.23.200.160/30, em que o endereço mais baixo é do router do ISP2.
- Em cada edifício das filiais estão previstos:

Prova sem consulta. Duração: 2h00min

- 10 APs Wi-Fi para dar acesso em qualquer ponto do edifício a 30 estações móveis;
- 4 Ethernet switches a 10/100 Mb/s, com 48 portas RJ45 e suporte de "Inline Power";
- 4 VLANs (para além da VLAN1 que se pretende acessível) com 20 estações na VLAN10 para os serviços administrativos e gestão, 60 estações na VLAN20 para os terminais VoIP, 10 estações na VLAN30 para os servidores locais e 120 estações (já incluídas as estações móveis) na VLAN40 para os utilizadores comuns da rede.
- No edifício sede estão previstos:
  - 24 APs Wi-Fi para dar acesso em qualquer ponto do edifício a 120 estações móveis;
  - 16 Ethernet switches a 10/100/1000 Mb/s, com 48 portas RJ45 e suporte de "Inline Power";
  - 4 VLANs (para além da VLAN1 que se pretende acessível) com 96 estações na VLAN10 para os serviços administrativos e gestão, 300 estações na VLAN20 para os terminais VoIP, 30 estações na VLAN30 para os servidores de toda a empresa e 480 estações (já incluídas as estações móveis) na VLAN40 para os utilizadores comuns da rede.

Para resolver o problema de endereçamento da empresa QQCOISA Lda foi-lhe atribuído o bloco de endereços 200.16.124.0/22 e 200.16.128.0/22.

1. Qual o número mínimo de redes que utilizava para resolver o endereçamento da empresa? Explique porquê, indicando o respetivo tamanho dos blocos de endereços. *—o faz-se redes de acesso a ISP1 e 2SP2??*

2. *VLANs no endereçamento?* Assumindo a atribuição de endereços que fez na pergunta anterior, apresente os vários endereços de identificação da rede, de broadcast e as respetivas máscaras, para cada uma delas. *Máscara decimal? 255.255.255.0??*

3. Considerando o número de postos de trabalho indicado e assumindo que cada utilizador tem acesso a um posto de trabalho e um terminal VoIP, sendo o horário de trabalho das 9:00 até as 18:00, considere os seguintes padrões de tráfego:

- E-mail – cada utilizador envia em média 20 Mbyte por dia e recebe 80 Mbyte. Cada edifício tem um servidor de E-mail. O tráfego recebido tem o seguinte padrão: cerca de 70% tem origem no exterior e o restante é interno ao edifício. O tráfego enviado tem o seguinte padrão: cerca de 20%

Prova sem consulta. Duracão: 2h00min

destina-se a endereços internos ao edifício, sendo os restantes 80% para destinatários externos:

- Acesso Web – cada utilizador acede em média a 30 Mbyte de conteúdos da empresa e 120 Mbyte de conteúdos externos;
  - VoIP – em média cada utilizador consome no total 4Mbyte de tráfego de entrada e de saída, sendo 80% para o exterior;
  - SAP – só 10% dos utilizadores das filiais e 20% do edifício sede usam o SAP; as transações médias de dados são de 15 kbyte. Cada utilizador faz uma média de 20 transações diárias;
  - Backup – é transferido diariamente, a partir das 00:30 até às 06:30, dos servidores localizados no edifício sede para os servidores alojados nas instalações de um *Service Provider*, uma cópia de segurança dos documentos gerados localmente, com o volume total médio de 3 Gbyte.

✓ a) Qual o modelo de fluxos que caracteriza cada um destes fluxos na rede?

✓ b) Quais são as fronteiras importantes dos fluxos da rede da empresa?

c) Quantifique com valores aproximados os fluxos de E-mail, acesso web e SAP entre edifícios. *el 1000*

d) Discuta o débito disponibilizado nos acessos à Internet no edifício sede, tendo em consideração os valores obtidos na resposta à alínea anterior.

FIM

ExemploGrupo II

1. Para uma rede média e grande dimensão interessaria utilizar o protocolo OSPF. É baseado numa arquitetura link-state, isto é, utiliza métricas que atribuem pesos às ligações. O seu protocolo é ligeiro depois do algoritmo de Dijkstra para encontrar o caminho mais curto. Deve-se, é um protocolo complexo, mas eficiente, com convergência rápida. Assim, numa rede de média e grande dimensão este é um protocolo bom que responde de forma eficiente às alterações na rede.

2. O protocolo SNMP é utilizado para gerir dispositivos como routers, switchs, servidores, em redes IP. Uma rede gerida por SNMP consiste em 3 componentes chave: os dispositivos a gerir, o software que corre nestes dispositivos (agente) e o NMS (Network Management Station), o software que corre no dispositivo que gera a rede. Uma rede pode ter mais do que um NMS. O SNMP não define, por si só, que informações (variáveis) um sistema a ser gerido oferece. As variáveis a ser geridas são o tempo de operação, o contacto, nome, localização e modo de interfaces são definidas pelas MIBs (Management Information Bases). A MIB descreve a estrutura dos dados geridos de um subsistema. Para isso é usado um espaço de nomes hierárquico que contém os vários OID (Object Identifier). Cada OID identifica uma variável que pode ser lida ou alterada através do SNMP. Para a gestão das variáveis o SNMP consistia inicialmente (SNMPv1) em 5 PDUs (Protocol Data Unit) que eram get request, get next request, set request, response e trap.

A versão 3, SNMPv3, veio a crescentar mecanismos de segurança e melhorar a configuração remota. Esta versão fez assegurar confidencialidade (encriptação dos pacotes para evitar a sua captura por pessoas sem autorização), integridade (para garantir que um pacote não foi alterado ou a sua ordem modificada) e autenticação (para verificar que as mensagens são provenientes de uma fonte válida).

### 3. Problema da segurança. Indicar possíveis ameaças.

As versões 1 e 2 estão sujeitas a packet shifting da community string pois não implementam encriptação e esta é enviada em texto simples.

Todas as versões estão sujeitas a ataques de brute force ou ataques de dicionário para adivinhar o community string, string de autenticação...  
~~O SNMP é normalmente usado~~

As ameaças podem ser classificadas como:

1 - Ameaças Principais: Disfarce / autenticação da origem - o intruso assume a identidade do remetente; alterações da informação / integridade dos dados - alterações das mensagens em trânsito

2 - Ameaças Secundárias: alterações do fluxo das mensagens - a sequência é alterada; exposição / confidencialidade dos dados - informação privilegiada é obtida por espiamento.

3 - Ameaças de menor importância: negação de serviço; análise de tráfego - os padrões de tráfego são examinados numa tentativa de se obter informação sensível

### 4. MIB RMON

MIB RMON (Remote Monitoring) permite a troca de dados de monitorização da rede entre vários sistemas. Funciona em cliente/servidor onde os equipamentos monitorizados, sondas RMON, têm instalado um software que recolhe informação e analisa pacotes. Estas sondas atuam como servidores e as aplicações de gestão como clientes. Tanto a configuração dos agentes como a coleta de informação usam SNMP mas em RMON as sondas têm mais responsabilidades em recolher dados e processar a informação, o que reduz o tráfego SNMP e a informação só é transmitida quando pedida, o que reduz o polling. No caso de haver mais que um NMS a sonda pode ser configurada para alejar concorrentemente os diferentes NMS.

### 5. PLANEAMENTO

a) Requisitos de Planeamento → UAFR

- Requisitos dos utilizadores
  - 1 n aplicações
  - 1 n equipamentos
  - 1 n rede

### c) Aplicações relativamente ao atraso

Tempo real (teleconferência)

Não são em tempo real

L1 Interativas { bulk (TELNET)

bursts (FTP)

L0 Assíncronas (e-mail)

### e) Implicações da introdução de procedimentos de gestão da rede

Impacto na capacidade do sistema, diminuindo o desempenho. É possível até utilizar equipamento dedicado atel.

## ② Áreas funcionais do modelo OSI - FCCDS

- 1 - Gestão das falhas
- 2 - Contabilização
- 3 - Configurações
- 4 - Desempenho
- 5 - Segurança

## ③ PLANEAMENTO

### a) SLA

Service Level Agreement, é a formalização do OS num contrato entre o cliente e o operador e estabelece os requisitos mínimos que devem ser fornecidos. Caso não seja cumprido o operador deve ser penalizado mas para isso é preciso monitorizar.

## ④ Explicar o que é uma MIB privada

MIB é uma especificação standard de monitorização que permite a troca de dados de monitorização entre sistemas. A MIB especifica os elementos de dados que um sistema precisa de ter, as operações permitidas em cada variável.

A MIB privada é aquela que contém objetos definidos por outras organizações. Fornece informações específicas dos equipamentos que estão a ser geridos assim como a configuração. É necessário que esta informação esteja no manager e no agente residente no sistema que se pretende gerir.

## PLANEAMENTO

### ① Requisitos de utilizador

Requisitos tratados com o utilizador, altamente relacionados com a performance, o atraso, a fiabilidade, a capacidade. Prontidão, interatividade, apresentação, adaptabilidade, funcionalidade, fiabilidade, custo, escalabilidade, suporte, segurança.

### ② Requisitos de rede

Capacidade de adaptar / corrigir / expandir o que já existe - atualizações. Ter em conta dependências e limitações por localizações. Dependências escalares, limitações de performance e dependências de interoperabilidade.

### ③ Requisitos de gestão

Monitorização, gestão de protocolos, características a monitorizar, in-band ou out-band, gestão centralizada ou distribuída, performance

### ④ factores de avaliação do desempenho da rede

- BW → capacidade de transporte
- Taxa transmissões → throughput
- Taxa efetiva → Goodput

### ⑤ Tipos de fluxos

Individual / composto / backbone

### ⑥ Modelos de fluxos

- peer-to-peer
- cliente-servidor
- cliente-servidor hierárquico
- computação cooperativa
- computação distribuída

## Perguntas teóricas

### 1º teste

1. Disponibilidade é a percentagem que indica o tempo em que um sistema está em funcionamento.
2. Uma estação de rede pode ter vários IPs e vários MACs. Por virtualização ou pode ter os endereços MAC trocados por protocolos. Ao ter vários MACs terá a vários endereços IP.
3. Detecção de fluxos na rede - detectar a fonte e o destino.
4. Computação cooperativa, os utilizadores e aplicações não são similares nos requisitos. Essa é a cliente-servidor hierárquico (DNS)
5. Análise de requisitos de capacidade: (débito)
  - do ponto de vista do atraso: tempo real (interativas / assíncronas) e não são em tempo real
6. last-mile: desde as infraestruturas até à casa do assinante
7. MTBF: mean time before failure  $\rightarrow$  tempo entre avarias  
MTTR: mean time to ~~repair~~  $\rightarrow$  tempo de avaria
8. Telnet  $\rightarrow$  do ponto de vista do atraso é interativa (não é em tempo real)
9. Monitorização out-band: é criada uma rede à parte para gestão e segurança in-band: a gestão utiliza a mesma rede do tráfego de produção
10. Escalabilidade: parâmetro que avalia a capacidade de crescimento de uma solução

### 2º teste

1. Quando o switch ethernet processa tramas e o endereço MAC não está na tabela, faz o envio para todas as portas menos a de origem.
2. Uma trama não pode ser fragmentada. Os pacotes podem ser fragmentados.
3. Repetidor de nível 1  $\rightarrow$  reconhece sinais elétricos apenas
4. Usando um router/switch o admin pode fazer encaminhamento seletivo de pacotes/tramas.

5. Agregar redes

rede 1	224.11.63/24	} $\Rightarrow$ 224.11.63.0
rede 2	224.11.159/24	

00111111  
 | 00111111

Possível { 224.11.64/24  
          | 224.11.65/24

Solução: 224.11.64/23  
Mas 224.11.64/23 pertence à rede multihomed  
usar 223

6. Endereço IPv6 128 bits hexadecimal ou MAC 48 bits hexadecimal
7. OSPF é um protocolo de routing interior Link-state
8. Protocolo IGP é interior, OSPF ou RIP
9. Last-mile - limitação da conectividade desde as infraestruturas até à casa do cliente.
10. Fluxos - indispensável conhecer a origem e o destino (não a direção)
11. SNMP - 3 operações: set, get, trap

### Problema - slide 36

bloco 200.23.48.121 usar o menor número possível de endereços  
do bloco

0011	0000	0000 000
.48		256
blocos disponíveis		

Para os 200 estagiões  
200.23.48.0 até 200.23.48.255 (256) /24

✓

180 pc's  $\Rightarrow$  200.23.49.0 até 200.23.49.255 (256) /24

110 pc's  $\Rightarrow$  200.23.50.0 até 200.23.50.127 (128 bits) /25

Filial B

Empresa A  $\Rightarrow$  60+R+R+B  $\Rightarrow$  200.23.50.128 até 200.23.50.191 /26

64 bits

Filial B  $\Rightarrow$  56+R+R+B  $\Rightarrow$  200.23.50.192 até 200.23.50.255 /26

64 bits

SEDE:  $\Rightarrow$  20+R+R+B  $\Rightarrow$  200.23.51.0 até 200.23.51.31 /27

32 bits

Filial B  $\Rightarrow$  20+R+R+B  $\Rightarrow$  200.23.51.32 até 200.23.51.63 /27

32 bits

FDDI  $\Rightarrow$  3+R+B  $\Rightarrow$  200.23.51.64 até 200.23.51.71 /29

8 bits

Empresa B  $\Rightarrow$  2+R+B  $\Rightarrow$  200.23.51.72 até 200.23.51.75 /30

4 bits

## Exame Exemplo

### GRUPO I

1. Verdadeiro: comutador Ethernet ... o endereço MAC ...
2. MIB privada basta estar no Agente Residente ??
3. Falso. Um trap SNMP é gerado pelo agente sempre que é produzida uma alteração numa variável monitorizada no ~~agente~~.
4. Na Análise de Requisitos está identificado o problema do "last-mile" como sendo a limitação da utilização da largura de banda disponível entre a infraestrutura do operador e a casa do cliente.
5. Falso. O MTBF é um parâmetro que é expresso em unidades de tempo e representa o tempo entre avisos, quando poderá ocorrer uma falha.
6. Falso. Na Análise de Requisitos devem ser considerados dois tipos de aplicações do ponto de vista de atraso, as aplicações de tempo real e as que não são de tempo real
7. O OSPF é um protocolo de routing do tipo ~~DTP~~ link-state mais utilizado na Internet devido à sua simplicidade, por suportar endereços de máscara variável, ter rápida convergência e ser um standard do IETF.
8. A disponibilidade tem um valor percentual e representa a probabilidade de um sistema / equipamento funcionar sem falhas.
9. No protocolo SNMP são previstas três operações básicas: set, get, trap.
10. O BGP4 é um protocolo de routing do tipo EGP e pode ser usado para trocar informações de routing entre routers de diferentes sistemas Autônomos.

### GRUPO II

1. OSPF é um protocolo link-state que usa o conceito de áreas (backbone + outras e de agregados). É standard IETF, tem baixo overhead daí a sua pertinência em redes de média e grande dimensão, faz partilho de carga e tem rápida convergência. As tabelas de routing são construídas dentro de cada área através de Multicast Hello packets e todas as áreas devem ser contíguas ao backbone. Isto minimiza o tamanho das tabelas de routing. No caso de uma alteração, esta apenas se faz sentir no nível da área. Outro protocolo é o BGP4, mais utilizado no caso de routing externo, ou seja para routing efetuado entre diferentes AS. O BGP4 constrói e gera uma tabela específica que é estudada pelo router para forwarding. A informação destas duas tabelas pode ser redistribuída. O BGP4 seleciona o melhor caminho

e inserir - e na tabela de routing IP. BGP4 tem rápidas convergências e é baseado no paradigma Least Hop, incluindo também autenticações.

2. O SNMP é um protocolo de gestão que permite operações de leitura, escrita trap. O SNMPv1 é baseado em TCP/IP cujas entidades são o gestor e o agente, o protocolo e a informação de gestão. Cada nó gerível é representado por um conjunto de variáveis. O trap ocorre quando o agente envia um aviso de ao manager devido a uma alteração numa das variáveis controladas pelo manager. O SNMPv1 apresenta limitações ao nível do polling, não sendo adequado para grandes quantidades de informação, as mensagens de trap não são confirmadas e a autenticação é trivial. O SNMPv2 traz novos tipos de dados, consensões textuais, facilitam a transferência de grandes quantidades de dados, são introduzidas novas macros. O SNMPv3 contempla agora quatro áreas de segurança, a autenticação, a privacidade, a autorização e controlo de acesso e a capacidade de configuração e administração remota. Existe uma nova entidade composta por duas peças: o motor SNMP e as aplicações

3. A segurança em SNMP é importante para a proteção da informação, o controlo de acesso aos recursos, a gestão centralizada ou distribuída, os níveis hierárquicos de acesso, o registo de eventos (logging) e a análise dos logs. No caso do SNMPv1 a autenticação é trivial e as mensagens de log trap não eram confirmadas. No SNMPv3 é feito o melhoramento da parte da segurança ao nível da autenticação, da privacidade, do controlo de acesso e a configuração e administração remota que pretende-se uma arquitetura modular que permita uma fácil expansão, permitindo no futuro novos protocolos de segurança, por exemplo. As ameaças podem ser principais: desfarre/autenticação de origem (o intruso assume a identidade do remetente para ganhar os seus privilégios), a alteração da informação/integridade dos dados (alterações das mensagens trocadas); ameaças secundárias são a alteração do fluxo das mensagens (a sequência é alterada/reordenada, as mensagens são atrasadas ou repetidas), a exposição/confidencialidade dos dados (informação privilegiada é obtida por espiagem das mensagens trocadas entre dois motores SNMP); outras ameaças de menor importância como a negação do serviço (negarão a utilizadores autorizados) e a análise do tráfego (padrões de tráfego examinados numa tentativa de obter informação sensível).

4. Uma RMON MIB é uma MIB de monitorização remota feita por uma unidade RMON. Permite off-line operation para resolver o problema do polling

permite proactivo monitoring, onde o monitor pode monitorizar e registar instantaneamente a rede, caso tenha recursos para tal; deteta e reporta problemas; value-added-data, o monitor analisa a informação recolhida na sua sub-rede, libertando o NMS; multiple managers, a rede pode ter mais do que um NMS e o monitor pode estar configurado para dialogar concorrentemente com os diferentes NMS.

5.

a) Requisitos de performance (reliability, availability, capacidade e delay) requisitos do utilizador (timeliness, interactivity, reliability, availability, throughput, adaptabilidade, segurança, custo, funcionalidade, escalabilidade); requisitos de aplicação (mission-critical, rate-critical, real-time and interactive) RMA (Reliability, maintainability, availability); aplicações-capacidade; rate-critical, best-effort; aplicações delay (real-time, non-real-time - interactive burst, interactive bulk, asynchronous); requisitos do equipamento (tipo, performance, localização); requisitos da rede (escalabilidade, localização, performance, rede, interoperabilidade); requisitos de gestão da rede (fazer as tarefas de gestão); requisitos financeiros (orçamento); requisitos técnicos (escalabilidade, disponibilidade, performance, segurança, gestão, usabilidade, adaptabilidade, peso)

b) localização dos dispositivos, para se determinar os fluxos da rede

c) Aplicações em tempo-real (ex: teleconferência); aplicações que não são em tempo-real;

- Interactive burst (ex: Telnet)
- Interactive bulk (ex: FTP)
- Assíncronas (ex: SMTP)

d) Problemas last-mile dizem respeito a falhas ao nível do equipamento do cliente. Problemas last-mile dizem respeito a falhas entre a infraestrutura do operador e a casa do cliente.

e) Há que tomar a decisão entre gestão in-band, isto é, o tráfego de gestão partilha a rede de produção ou gestão out-band, onde é criada uma rede separada para o tráfego de gestão da rede.

### Grupo III

1. Qual o modelo de fluxos para cada um destes fluxos na rede?

Email tem o modelo cliente-servidor. O acesso Web é cliente-servidor.

VoIP é peer-to-peer. SAP é computação cooperativa (entre servidores e gestores). O fluxo de backup é cliente-servidor.

Entre GW1 e ISP1 / GW1 - ISP2 / ISP1 e GW2 / ISP1 e GW3

2. Fronteiras: 2 WAN's, uma para o ISP1 e outra para o ISP2.

A rede da sede, da filial A e da filial B

3) Quantificar com valores os fluxos de Email, web, VoIP e SAP entre edifícios.

Email:

No edifício sede temos 480 utilizadores, o tráfego enviado p/dia é 14800 Mbytes e recebido 12000 Mbytes p/8 horas

O tráfego recebido é 30/70 e o enviado é 60/40 (este é claramente um fluxo de backbone).

No Filial 1 e 2 temos 120 utilizadores

O tráfego enviado é 1200 Mbytes e o recebido é 3000 Mbytes.

Acesso Web:

No Sede

4.

### Grupo III

Sede → Ethernet 40Mbps

Filiais → Ethernet 20Mbps

2x **[Filiais]** ↳ 10 AP's wi-fi  
30 estações móveis

**[Sede]** ↳ 24 AP's wifi  
120 estações móveis

4 VLANs

VLAN10 → 20 estações  
→ admin + gestão

VLAN20 → 60 estações  
→ VoIP

VLAN30 → 10 estações  
→ serv. locais

VLAN40 → 120 estações (90 + 30 móveis)  
→ utilizadores comuns

4 VLANs

VLAN10 → 96 estações  
→ admin + gestão

VLAN20 → 300 estações  
→ VoIP

VLAN30 → 30 estações  
→ servidores

VLAN40 → 480 estações (360+120H)  
→ utilizadores

- Cada utilizador tem um posto e um terminal móvel

• E-mail → 10Mbyte / dia send } 8 horas  
25Mbyte / dia receive }

tráfego recebido: 20% Ext / 30% Int

tráfego enviado: 60% Int / 40% Ext

• Acesso Web → 10Mbyte da empresa  
40Mbyte ext

• VoIP → 2Mbyte entrada  
2Mbyte saída

• SAP → 10% nas filiais } transações de 15Kbyte x 20 p/dia  
20% na sede

• Backup → das 00:00 às 07:00 da sede → FSP → 5Gbyte

3. Postos nas filiais:

→ 20 admin /gestão

→ 60 VoIP

→ 120 users

Postos na sede

→ 96 admin

→ 300 VoIP

→ 480 users

• E-mail:

$$\frac{900K}{28,8} = 31,25 \text{ kbytes/s}$$

$$\text{Recebida na filial: } \frac{25M \times 0,3 \times 120}{8 \times 3600} = 52,8 \text{ bytes/s}$$

$$\text{Recebida na sede: } \frac{25M \times 0,3 \times 480}{8 \times 3600} = 228,8 \text{ bytes/s} \quad 125 \text{ kbytes/s}$$

$$\text{Enviada na filial: } \frac{10M \times 0,6 \times 120}{8 \times 3600} = 25 \text{ kbytes/s}$$

$$\text{Enviada na sede: } \frac{10M \times 0,6 \times 480}{8 \times 3600} = 100 \text{ kbytes/s}$$

• Web

$$\text{Filial: } \frac{40M \times 120}{8 \times 3600} = 166,7 \text{ kbytes/s}$$

$$\text{Sede: } \frac{40M \times 480}{8 \times 3600} = 666,7 \text{ kbytes/s}$$

• VoIP:

$$\text{Filial: Entrada = Saída} = \frac{2M \times 60}{8 \times 3600} = 4,17 \text{ kbytes/s}$$

$$\text{Sede: Entrada = Saída} = \frac{2M \times 300}{8 \times 3600} = 20,83 \text{ kbytes/s}$$

• SAP:

10% utilizadores das filiais = 12

20% sede = 96 utilizadores

$$\cdot \frac{15K \times 12 \times 20}{8 \times 3600} = 125 \text{ bytes/s}$$

$$\frac{15K \times 96 \times 20}{8 \times 3600} = 1 \text{ Kbytes/s}$$

4. Débito:

Sed -> ~~10MB/s from hits~~ → 5MByte/s

Traffego total diário: ~~725K + 100K + 666,7K + 2x20,83K + 1K =~~  
= 932,9 kByte/s ⇒ sobredimensionada

Backup

$$\frac{5000 \text{ M}}{7 \times 3600} = \frac{5000 \text{ K}}{25,2} = \underline{\underline{198,4 \text{ kByte/s}}} \Rightarrow \text{sobredimensionada}$$

O backup podia ser feito durante o dia!

Exame 2012/2013

Grupo III

Acesso ao ISP1  $\Rightarrow 84.155.41.65/30 \Rightarrow GW1$

$84.155.41.129/30 \Rightarrow GW2$

$84.155.41.193/30 \Rightarrow GW3$

ISP2  $\Rightarrow 195.23.200.160/30 \Rightarrow 1^{\text{a}} \text{ e } 2^{\text{a}} \text{ router do ISP2}$

Filiais:

{ 10 AP's Wi-Fi  $\Rightarrow 30$  estações móveis  
4 switches 10/100 Mb/s  $\Rightarrow 48$  portas  
VLAN 10  $\Rightarrow 20$  estações admin/gestão ✓  
VLAN 20  $\Rightarrow 60$  n VoIP ✓  
VLAN 30  $\Rightarrow$  servidores locais ✓  
VLAN 40  $\Rightarrow 120$  estações (90+30M) ✓

Sede:

{ 24 AP's Wi-Fi  $\Rightarrow 120$  estações móveis  
16 switches 10/100/1000 Mb/s  $\Rightarrow 48$  portas  
VLAN 10  $\Rightarrow 96$  estações admin ✓  
VLAN 20  $\Rightarrow 300$  n VoIP ✓  
VLAN 30  $\Rightarrow$  servidores ✓  
VLAN 40  $\Rightarrow 480$  estações (360+120M) ✓

1.

Endereçamento:  $200.16.124.0/22$  e  $200.16.128.0/22$ .

200.16.0111.11 00 0 0  
256

200.16.1000.00 00 0

1º bloco  $\Rightarrow 480$  estações <sup>sede</sup>  $\Rightarrow$  De 200.16.124.0/22 até 200.16.125.255/22  $\Rightarrow 512$  endereços

2º bloco  $\Rightarrow 300$  estações <sup>sede</sup> VoIP  $\Rightarrow$  De 200.16.126.0/22 até 200.16.127.255/22  $\Rightarrow 512$  endereços

3º bloco  $\Rightarrow$  ~~120 estações~~ filial A

~~120 estações~~  $\Rightarrow$  De 200.16.128.0/25 até

200.16.128.127/25  $\Rightarrow 128$  endereços

4º bloco  $\Rightarrow$  120 estações filial B  $\Rightarrow$  De 200.16.128.128/25 até 200.16.128.255/25  $\Rightarrow$  128 endereços

- 5º bloco  $\rightarrow$  60 VoIP da filial A  $\Rightarrow$  200.16.129.0/26 até 200.16.129.63/26 = 64 endereços  
 6º bloco  $\rightarrow$  60 VoIP da filial B  $\Rightarrow$  200.16.129.64/26 até 200.16.129.127/26 = 64 endereços  
 7º bloco  $\Rightarrow$  96 estações admin  $\Rightarrow$  De 200.16.129.128/26 até 200.16.129.255/25  
 $\Rightarrow$  128 endereços  
 8º bloco  $\Rightarrow$  20 estações admin filial A  $\Rightarrow$  200.16.130.0/26 até 200.16.130.31/26 = 32 endereços  
 9º bloco  $\Rightarrow$  20 estações admin filial B  $\Rightarrow$  De 200.16.130.32/26 até 200.16.130.63/26 = 32 endereços

servidores locais: ~~Web, SAP, Bases de dados, Email, DNS, proxy, BGP, Backup~~  
 $\Rightarrow$  blocos de 8 endereços  $\times 3$

Para a sede: De 200.16.130.64/29 até 200.16.130.71/29 = 8 endereços  
 Para a Filial A: De 200.16.130.72/29 até 200.16.130.79/29 = 8  
 Para a Filial B: De 200.16.130.80/29 até 200.16.130.87/29 = 8

Redes delegadas a ISP 1:

GWT + RFB - 0.84.185.41.68/30 até 0.84.155.41.68/30

VLAN1 sede = 24 AP's + 16 switches + 1 router = 41 endereços

2.

#	Rede / função	Rede	broadcast	máscara
1	480 estações da sede	200.16.124.0	200.16.125.255	255.255.252.0
2	300 " VIP sede	200.16.126.0	200.16.127.255	255.255.252.0
3	120 estações filial A	200.16.128.0	200.16.128.127	255.255.255.128
4	120 " filial B	200.16.128.128	200.16.128.255	255.255.255.128
5	60 VoIP filial A	200.16.129.0	200.16.129.63	255.255.255.192
6	60 VoIP filial B	200.16.129.64	200.16.129.127	255.255.255.192
7	96 admin sede	200.16.129.128	200.16.129.255	255.255.255.128
8	20 admin filial A	200.16.130.0	200.16.130.31	255.255.255.224
9	" " " " B	200.16.130.32	200.16.130.63	255.255.255.224
10	servidores sede	200.16.130.64	200.16.130.71	255.255.255.248
11	servidores filial A	200.16.130.72	200.16.130.79	255.255.255.248
12	servidores filial B	200.16.130.80	200.16.130.87	255.255.255.248
	VLAN1 sede			
	VLAN1 filial A			
	VLAN1 filial B			