

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.

É quando não consegue encontrar o endereço destino na sua tabela de encaminhamento. Intencionalmente é encaminhada para todas as interfaces portadoras da VLAN.

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.

- *) O problema do "last-mile" é futuramente servir e performance à interface do sistema através das suas aplicações e utilizadores.

- F 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.

O problema do last-mile consiste na dificuldade em fazer chegar uma infraestrutura, uma rede de serviços até um campus ou um edifício, ou seja, marcar até ao ponto final a que está na linha.

- F 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
ocorrido
entre duas
falhas em
unidades de
tempo

MTBF - Mean Time Between failures. Este valor expresso em unidades de tempo indica quando podemos esperar uma falha no aparelho.

- F 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.

Rate-critical applications - aplicações que precisam uma disponibilidade previnindo falhas de grande magnitude.
Best-effort applications - não garantem que a informação seja entregue às utilizações podendo obter uma alta variação e um tempo de entrega dependente do tráfego.

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.

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

Normalmente significa o tempo em que a rede está operacional. É a % de tempo por hora/dia/semana/ano em que o sistema está avarado.

Prova sem consulta. Duração: 2h00min

Exemplo

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

Nas operações de set, poll e getbulk é necessário especificar o nome do objecto. No entanto, no caso de trap, este nome é ignorado.

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.

O BGP4 é um protocolo de routing que opera entre routers de diferentes sistemas autónomos.

Quando se usa o BGP4 para trocar informações de routing entre routers de diferentes sistemas autónomos, é necessário que exista uma ligação entre os sistemas autónomos.

Quando se usa o BGP4 para trocar informações de routing entre routers de sistemas autónomos que fazem parte do mesmo sistema autónomo, é necessário que exista uma ligação entre os routers.

Quando se usa o BGP4 para trocar informações de routing entre routers de sistemas autónomos que fazem parte do mesmo sistema autónomo, é necessário que exista uma ligação entre os routers.

Quando se usa o BGP4 para trocar informações de routing entre routers de sistemas autónomos que fazem parte do mesmo sistema autónomo, é necessário que exista uma ligação entre os routers.

Quando se usa o BGP4 para trocar informações de routing entre routers de sistemas autónomos que fazem parte do mesmo sistema autónomo, é necessário que exista uma ligação entre os routers.

Quando se usa o BGP4 para trocar informações de routing entre routers de sistemas autónomos que fazem parte do mesmo sistema autónomo, é necessário que exista uma ligação entre os routers.

Quando se usa o BGP4 para trocar informações de routing entre routers de sistemas autónomos que fazem parte do mesmo sistema autónomo, é necessário que exista uma ligação entre os routers.

Quando se usa o BGP4 para trocar informações de routing entre routers de sistemas autónomos que fazem parte do mesmo sistema autónomo, é necessário que exista uma ligação entre os routers.

Quando se usa o BGP4 para trocar informações de routing entre routers de sistemas autónomos que fazem parte do mesmo sistema autónomo, é necessário que exista uma ligação entre os routers.

Quando se usa o BGP4 para trocar informações de routing entre routers de sistemas autónomos que fazem parte do mesmo sistema autónomo, é necessário que exista uma ligação entre os routers.

Quando se usa o BGP4 para trocar informações de routing entre routers de sistemas autónomos que fazem parte do mesmo sistema autónomo, é necessário que exista uma ligação entre os routers.

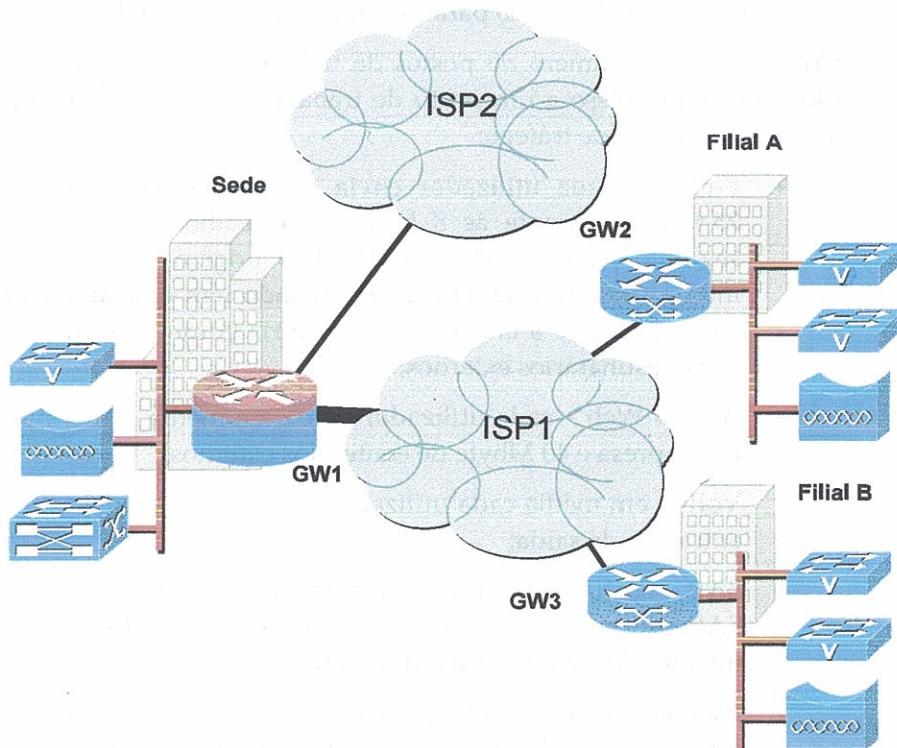
Quando se usa o BGP4 para trocar informações de routing entre routers de sistemas autónomos que fazem parte do mesmo sistema autónomo, é necessário que exista uma ligação entre os routers.

Quando se usa o BGP4 para trocar informações de routing entre routers de sistemas autónomos que fazem parte do mesmo sistema autónomo, é necessário que exista uma ligação entre os routers.

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

- ✓ 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.
- ✓ 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.

Prova sem consulta. Duração: 2h00min

Exemplo

- 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.
 4. Discuta o débito disponibilizado nos acessos à Internet no edifício sede, tendo em consideração os valores obtidos na pergunta anterior.

FIM

EXAME EXEMPLO → PGRE

- 1) Protocolos de Routing mais importantes para gerar das redes ou acervo a uma intra-estrutura de rede média e grande dimensão

→ Routing Interno → OSPF, EIGRP, IBGP, IGRP,
→ Routing Externo → IS-IS
BGP4

- Protocolos de Routing:

RIP, HELLO, IGRP, OSPF, IS-IS, EGP, BGP4

- Para redes de média e grande dimensão os protocolos baseados em distância-vektor adicionais não servem:

OSPF, EIGRP, IS-IS

- OSPF - Open Shortest Path First - é um protocolo standart pelo IETF, podendo ser utilizado por qualquer fabricante, garantindo heterogeneidade. Este protocolo utiliza o protocolo de routing link-state, sendo desta forma mais eficiente, contudo mais exigente na capacidade de processamento.
- No protocolo de routing link-state os nós anunciam pela rede apenas os seus pacotes link-state para informar os outros sobre o seu estado. Seguidamente os LSDBs recebidos dos nós vizinhos vão ser utilizados para construir um modelo global da rede e uma tabela de routing. Os melhores caminhos são calculados utilizando o algoritmo de Dijkstra.
- EIGRP - Enhanced IGRP - é um protocolo que utiliza o protocolo de routing link-state mas com diferenças face ao original: em vez de enviar a sua tabela de routing por completo apenas envia partes da tabela que os outros nós ainda não conhecem. A vantagem disto é descurpar alguma largura de banda, sendo importante esta modificação no caso de redes de média e grande dimensão.
- IS-IS - protocolo standart OSI semelhante ao OSPF mas o protocolo OSPF foi desenvolvido para rede IP, o IS-IS é um protocolo da camada 3 que corre em cima do IP, visto que é um protocolo OSI da camada 3.

• Comparação:

→ OSPF e IS-IS são protocolos standardizados (OSPF → IETF
IS-IS → OSI/IETF)

EIGRP é uma evolução do IGRP e é proprietário da Cisco

→ Os três protocolos têm um tempo de convergência baixo ≈ 1s

→ Só complexo

→ OSPF calcula o custo das rotas da seguinte maneira:

$$\text{COST} = \frac{\text{interface BW}}{\text{interfaz BW}}$$

→ EIGRP calcula e na largura

a métrica com base nos artigos de banda (velocidade)

→ IS-IS calcula métrica atribuindo um peso de 10 a cada ligação

→ Tanto o OSPF como o IS-IS são caracterizados pela divisão da rede em áreas, mas apenas o OSPF precisa que as áreas dividem entre todos os adjacentes à área 0.

→ OSPF é meia-ponta: mais escalável e, para os mais meia-pontas, mais routers

funcionando, mas IS-IS é mesmo meia-ponta conseguindo que o OSPF é mais complexo.

→ O B-IS, no entanto,

②. caracterizar o protocolo SNMP, fazendo referência à evolução das várias versões. Alterações importantes com SNMPv3.

O protocolo SNMP é um Internet Standard protocol utilizado para gerir dispositivos como routers, switches, servidores, em redes IP.

Uma rede gerida por SNMP consiste em 3 componentes chave: dispositivos a gerir, o software que corre nestes dispositivos (agent) e o NMS (Network Management Station), o software que corre no dispositivo que gera a rede. Uma rede pode ter mais de um NMS.

O SNMP por si só não dispõe que informações (variáveis) um sistema a ser gerido oferece. As variáveis a serem

guidas: tempo de operação, contacto, nome, localização e nº de interfaces, só de finidas pelas MIBs (Management Information Bases). A MIB descreve a estrutura dos dados genéricos de um subsistema de um dado dispositivo. Para isso é usado um espaço de nomes hierárquico que contém vários OID (Object Identifiers). Cada OID identifica uma variável que pode ser lida ou alterada através do SNMP.

Para a gestão destas variáveis o SNMP conta inicialmente (SNMPv1) em 5 PDUs (Protocol Data Unit) principais:

→ Get Request: pedido manager-to-agent para ir buscar o valor de uma das variáveis. Os valores requisitados são recuperados no agente através de uma operação get-request e este envia uma resposta ao manager com os valores pedidos.

→ Get Next Request: pedido manager-to-agent para descobrir as variáveis disponíveis para gestão e os seus valores. Retorna uma resposta à próxima variável da MIB.

→ Set Request: pedido manager-to-agent para alterar o valor de uma variável na lista de variáveis. Uma resposta é devolvida com os novos valores através das variáveis a alterar.

→ Response (Get Response no SNMPv1) - Responsável por informar respostas dos pedidos get e set do manager. O sentido é agent-to-manager. Esta PDU contém 2 campos para informar end. O ACK enviado na resposta ao Inform Request (SNMPv2) também é deste tipo.

→ Trap - notificação do agente para o manager a indicar a ocorrência de um evento significativo (valor de uma variável atingiu um dado limite, por exemplo). Esta mensagem é enviada automaticamente para o manager.

Na versão 2 a performance deste protocolo foi melhorada. Além de serem alterados os formatos dos PDUs existentes foram adicionadas mais duas:

→ Get Bulk Request - versão otimizada do Get Next Request. Permite pedir logo várias instruções do Get Next Request melhorando a eficiência das operações de percorrer e descobrir variáveis na MIB de um agente.

→ Inform Request: utilizada essencialmente na comunicação manager-to-manager mas também pode ser usada na agent-to-manager. No fundo consiste numa trap que exige como resposta um ACK para se confirmar a execução da trap.

A versão 2 tentou também implementar mecanismos de segurança no SNMP (cujo único mecanismo era a community string que é enviada em texto sem qualquer encriptação), mas não chegou a conseguir pois os mecanismos propostos tornariam o SNMP um protocolo mais complexo e uma das suas grandes vantagens é a sua simplicidade.

A versão 3 veio adicionar mecanismos de segurança ao SNMP e melhorar a configuração remota. Estas alterações introduzidas na versão 3 vieram asseguradas:

→ confidencialidade - encriptação dos pacotes para evitar captura de pacotes por terceiros / autorização (packet sniffing)

→ integridade - assegurada para garantir que um pacote não foi alterado ou a sua ordem modificada ao longo do percurso. Inclui ainda um mecanismo de proteção opcional para envio dos pacotes

→ autenticação - para verificar que as mensagens são provenientes de uma fonte válida.

③. caracterizar o problema da segurança num sistema ~~SNMP~~ de gestão baseado no SNMP.

→ As versões 1 e 2 do SNMP estão sujeitas a packet sniffing da community string pois não implementam encriptação e esta é enviada em texto simples nos pacotes. Isto é resolvido na versão 3 com encriptação.

→ Todas as versões do SNMP estão sujeitas a ataques de força bruta e ataques de dicionário para adivinhar a community string, string de autenticação, strings de encriptação, chaves de autenticação e de encriptação pois não implementam um handshake de desafio-resposta

→ O SNMP é usado normalmente sobre UDP que é um protocolo não orientado às ligações e vulnerável a ataques de IP spoofing (o atacante envia um pacote com o IP de um ponto legítimo). O mecanismo de autenticação introduzido na versão 3 resolve este problema

um dos problemas da community string e o administrador mais frequentes do SNMP é o fato de, por definição de rede como pública da rede não a alterar para "private"

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

uma MIB (Remote Monitoring) é uma especificação Standard de monitorização que possibilita a troca de dados de monitorização da rede entre vários sistemas. Uma implementação RMON funciona num estudo cliente/servidor onde os dispositivos monitorizados, chamados sondas RMON (RMON Probes) têm instalado um software de agente RMON que coleta pacotes. Estas sondas atuam como servidores e as aplicações de gestão da rede que comunicam com elas atuam como clientes. Tanto a configuração dos agentes como a colecção de informação usam SNMP, no entanto, RMON distingue-se de outros sistemas baseados em SNMP pois as sondas têm mais responsabilidade em relação ao dados e provêem a informação, o que reduz o tráfego SNMP e a informação só é transmitida para a aplicação de gestão quando pedida, em vez de a enviar automaticamente (continuous polling). Estes 2 factos permitem resolver o problema do polling, permitindo uma monitorização constante da rede pelas sondas (caso haja necessidade), como a sonda é que analisa a informação recolhida pelo NMS fica mais leve e no caso de ter mais de 1 NMS, a sonda pode ser configurada para atender convenientemente os diferentes NMS. É mais orientada para monitorizar equipamentos e pode precisar de equipamento dedicado para monitorizar a rede se operam dimidiados NMS.

5. Planeamento

a) Na análise de requisitos para o planeamento da rede há diferentes tipos de requisitos? Quais e como os organiza os requisitos para o planeamento de uma rede podem ser organizados da seguinte maneira:

→ Requisitos dos utilizadores - requisito como a pronunciado, interatividade, funcionalidade, segurança, fiabilidade, alcance futuro ou custo

→ Requisitos das aplicações - pacote ser do tipo Real-time, rate-critical ou mission-critical e que abordam os temas da fiabilidade, manutenção, disponibilidade, aplicações em tempo real ou aplicações que dependem da capacidade.

→ Requisitos dos equipamentos - tipo de equipamento, localização e performance

→ Requisitos de rede - Gestão de redes, objetivos técnicos como a disponibilidade, a performance e a segurança

b) Qual a importância da localização dos equipamentos na análise de requisitos?

Saber a localização é importante para determinar a ligação entre utilizadores, aplicações e rede. É importante para redes cujos componentes de sistema ou funções são dispersos.

A localização dos equipamentos é o 1º passo para determinar características do sistema no que toca a fluxos de tráfego.

c) Que tipo de aplicações distinguem na análise de requisitos relativamente a amos? Caracterize-as.

No análise de requisitos relativamente ao amos é possível identificar dois tipos de aplicações:

→ Aplicações em tempo real → telefonemas / videochamadas. Estas aplicações são muito sensíveis ao atraso. Neste tipo de aplicações é preferível perder alguma informação e/ou qualidade do que a informação chegar com um atraso tal que seja perniciosa aos utilizadores.

→ Aplicações que não são em tempo real → não há grande problema se a informação chegar com algum atraso. É mais importante que a informação chegue completa e segura.

- Interactivas

- burst → informação chega por picos → telnet
- bulk → informação de grande volume → backup → FTP

- Américas → insensíveis ao atraso e-mail.

d) Qual a diferença de aplicação dos problemas "last foot" e "last mile"?

Os problemas "last foot" e "last mile" são problemas existentes nos requisitos de equipamentos na área da performance. O "last mile" caracteriza-se por sendo a dificuldade em trazer intra-estrutura, rede e serviços para um campus ou edifício. Trazer até ao anfitrião o que se encontra na intra-estrutura original, como por exemplo: trazer fibra óptica até um condomínio.

O problema "last foot" é a dificuldade em trazer os serviços e a performance da interface de rede do aparelho até às suas aplicações e utilizadores. Por exemplo: cada de rede não tem capacidade para aceitar Gb, largamento e protocolos vários, diferentes desempenhos.

e) Quais as implicações da introdução de procedimentos de gestão da rede a considerar no projeto lógico e, posteriormente, na exploração da rede?

É necessário ter em atenção o impacto dos procedimentos de gestão nos equipamentos da rede, visto que há a possibilidade da componente de gestão começar a executar uma grande faia da capacidade do sistema, diminuindo o desempenho da rede. É costume até, quando necessário, utilizar equipamento dedicado para a gestão da rede.

Grupo I:

1. Falso! Quando um comutador Ethernet processa uma trama e o endereço MAC de destino é desconhecido nas suas tabelas de encaminhamento, a trama é encaminhada para todas as interfaces, excepto aquela que está ligada ao destino.
2. Verdadeiro! 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. Falso! Um trap SNMP é gerado pelo agente sem que seja produzida uma alteração numa variável monitorizada pelo agente.
4. F. "last mile" ... dificuldade em fazer chegar a infraestrutura de conectividade e serviços para dentro de um campus ou um edifício.
5. F. MTBF (...) não apresenta o tempo médio entre falhas de um sistema ou equipamento
6. F. do ponto de vista do amanu.
7. F. IGP - suporta end. de máscara variáveis.
8. F. não apresenta a probabilidade de um sistema estar operacional
9. F. Três operações básicas: set, get e trap
10. Verdadeiro!

GRUPO III

Sede → ethernet 40 Mb/s

Filiais → ethernet 20 Mb/s

Filiais:

→ { 70 APs Wi-Fi
30 estações móveis

→ 4 VLANs:

VLAN 10 → 20 estações
→ admin + gestão

VLAN 20 → 60 estações
→ terminais VoIP

VLAN 30 → 70 estações
→ serv. locais

VLAN 40 → 120 estações (já incluindo os móveis)
→ utilizações comuns

Sede:

→ { 24 APs Wi-Fi
120 estações móveis

→ 4 VLANs

VLAN 10 → 96 estações
→ admin + gestão

VLAN 20 → 300 estações
→ VoIP

VLAN 30 → 80 estações
→ servidores da empresa

VLAN 40 → 480 estações
→ utilizações comuns

→ Cada utilizador tem acesso a um porto de trabalho e a um terminal VoIP

- E-mail → 70Mbyte/dia send
25Mbyte/dia receive
8h.

Tráfego Móvel: 70% ext.
30% empresa

Tráfego enviado: 60% em P2P
40% externo

- Acesso Web → 10 Mbyte empresa
40 Mbyte externo

- VoIP → 2 Mbyte entrada
2 Mbyte saída

- SAP → 70% utilizadoresiais
20% " sedu

Transações médias: 15Kbyte
20 transações diárias

- Backup → 00:00 às 7:00
Sede p/ ISP
óptica segurança local
5 Gbyte.

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

E-mail → Cliente-Servidor → os fluxos entre clientes e servidores tendem a ser assimétricos

Acesso Web → Cliente-Servidor

VoIP → Peer-to-peer

SAP → Cliente-Servidor → transações financeiras

Backup → Cliente-Servidor

2. Quais são as montanhas importantes dos fluxos da rede da empresa?

Montanhas situadas nas ligações aos ISPs:

- entre GW1 e ISP1
- entre GW1 e o ISP2
- entre o ISP1 e a GW2
- entre o ISP1 e a GW3

3. Quantifique com valores aproximados os fluxos de e-mail, aceso Web, VoIP e SAP entre edifícios

Portas de trabalho nas filiais:

- 20 estações dos env. admin e gestão
- 60 estações de terminais VoIP
- 120 estações de utilizadores

Total: 200

Portas de trabalho na Sede:

- 96 estações dos env. admin. e gestão
- 300 estações dos term. VoIP
- 480 estações de utilizadores comuns

Total: 876

E-MAIL

- Envia 10Mbyte/dia
- Recebe 25 Mbyte/dia
- 8 horas
- Tráfego recebido
 - 70% externo
 - 30% interno
- Tráfego enviado
 - 60% interno
 - 40% externo

WEB

- 10Mbyte interno
- 40 Mbyte externo

BACKUP:

00:00 - 7h
cópia local
5 Gbyte

VOIP

- 2 Mbyte entrada
- 2 Mbyte saída

SAP

- 10% utilizadores fiéis
- 20% utilizadores saud
média 15K byte
- 20 /dia

utilizados:

→ 200 Filiais

→ 876 seds

E-mail:

$$\frac{25M \times 0,3 \times 200}{8 \times 3600} = 52 \text{ K byte/s, enviado filial}$$

$$\frac{25M \times 0,3 \times 876}{8 \times 3600} = 228 \text{ K byte/s, enviado sed}$$

$$\frac{10M \times 0,6 \times 200}{8 \times 3600} = 42 \text{ K byte/s, enviado filial}$$

$$\frac{10M \times 0,6 \times 876}{8 \times 3600} = 183 \text{ K byte/s, enviado sed}$$

WEB:

$$\frac{10M \times 200}{8 \times 3600} = 69 \text{ K byte/s, filial}$$

$$\frac{10M \times 876}{8 \times 3600} = 304 \text{ K byte/s, sed}$$

VoIP:

$$\frac{2M \times 200}{8 \times 3600} = 14 \text{ K byte/s enviado filial}$$

14 K byte/s enviado filial

$$\frac{2M \times 876}{8 \times 3600} = 61 \text{ K byte/s enviado sed}$$

61 K byte/s enviado sed

não é usado

SAP:

10% utilizadores fiúais = 20

20% utilizadores fiúais = 175

$$\frac{20 \times 15k \times 20}{8 \times 3600} = 20,83 \text{ byte/s} \rightarrow \text{fiúal}$$

$$\frac{20 \times 15k \times 175}{8 \times 3600} = 1823 \text{ byte/s.} \rightarrow \text{secu}$$

4. Discuta o débito disponibilizado nos acessos à internet

⇒ → Secu: 40 Mb/s → 5 M byte/s

→ Fiúais: 20 Mbit/s → 2,5 M byte/s

228 K byte/s → usado e-mail

183 K byte/s → enviado e-mail

304 K byte/s → acesso web

61 K byte/s → enviado VoIP

61 K byte/s → usado VoIP

+ 1823 byte/s → SAP

TOTAL: 839 Kbyte/s vs 5 M byte/s.

↳ A rede está sobdimensionada

→ O débito do SAP é tão reduzido que não atesta a dimensão dos fluxos da rede

→ Há capacidade para fazer o backup, quer no horário da noite como nas horas de expediente, visto que manter 5Gb durante 7 horas gera um fluxo de 200 Kbyte/s

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.

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

O endereço MAC de destino do pacote enviado pela estação de origem é o endereço MAC da estação de destino.

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

Na comunicação entre duas estações localizadas em LAN's distintas, um pacote pode ser fragmentado as vezes que forem necessárias e deve ser reconstruído pela estação de destino.

- F 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.

Prova sem consulta. Duração: 2h00min

F

4. O SNMP é uma solução de gestão de redes locais suportada nos protocolos de transporte TCP e UDP.

Apenas UDP

F

5. Na Análise de Requisitos devem ser consideradas dois tipos de aplicações do ponto de vista da capacidade, as aplicações interativas e as assíncronas.

Real-time e as Best-effort

Amano Real time

Non-real Time

Interativas

Assíncronas

P

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).

Apenas BGP

P

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 uma norma do IETF.

IGP

F

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.

a média de tempo necessário à reparação de um equipamento/máquina

tempo médio de reparação de uma falha de um sistema/equipamento

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 de gestão

10. O BGP4 é um protocolo de routing exterior do tipo *distance vector* e pode ser usado para trocar informação de routing entre routers dentro do mesmo Sistema Autónomo.

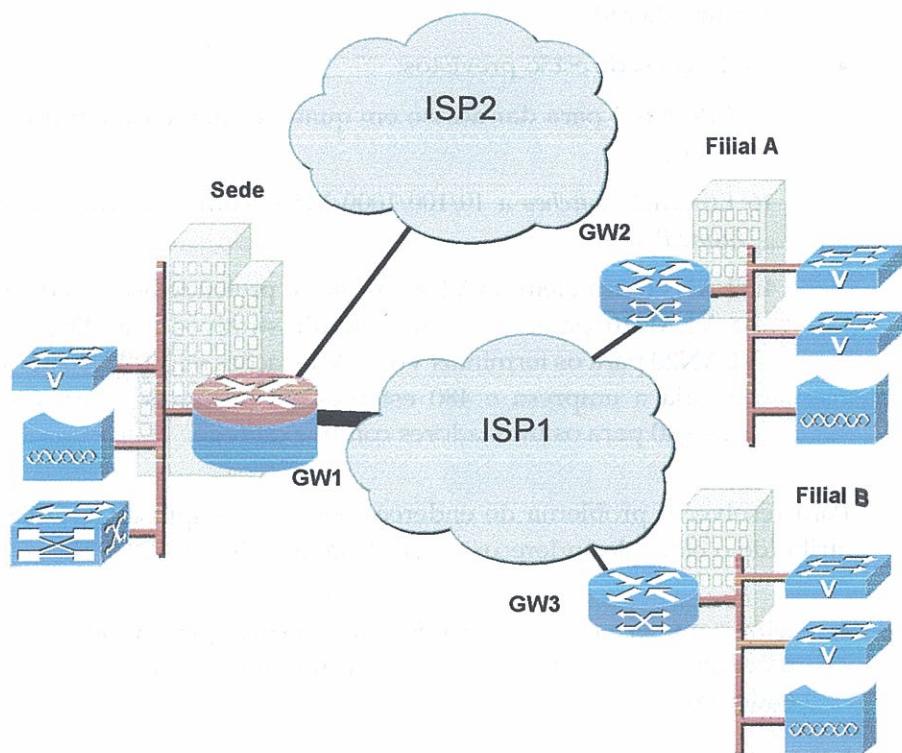
Prova sem consulta. Duração: 2h00min

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.
- ✓ 2. Apresente as áreas funcionais do modelo OSI de gestão de redes, descreva os procedimentos e objetivos para cada uma delas
- ✓ 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:
 - ✓ a) O que entende por SLA e qual a relevância que lhe reconhece?
 - ✓ b) Qual a importância da localização dos equipamentos na análise de requisitos?
 - ✓ c) Diga o que entende por um serviço de acesso à Internet com 99,50% de disponibilidade.
 - d) O que indica o valor do MTBF? Qual a sua relevância?

Prova sem consulta. Duração: 2h00min

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

FIM

卷之三

GRUPO I

1. Falso. O endereço MAC de destino.
2. Falso. (...) uma trama pode ser fragmentada quantas vezes forem necessárias (...) devem ser reconstituídas pelas estações de destino.
3. Falso. SNMPv3 → segurança
4. Falso. Apenas UDP
5. falso. ponto de vista do atacante
ou ponto de vista da capacidade (...) best-effort, rate-critical
6. falso. O BGP (...)
7. falso. IGP... Nodos TCP/IP... respondem ao mesmo protocolo.
8. falso... o tempo médio para reparar uma falha.
9. falso... quatro... e a informação de gestão.
10. v... su path vector

Grupo II

1. PEQUENA E, MÉDIA DIMENSÃO?

RIP, HELLO e IGRP

→ Baseados no algoritmo distance-vector, em vez de link-state visto que a sua complexidade é menor, apesar dos tempos de convergência não serem tão bons

→ Distance-Vector: consiste em ter vários nós da rede que enviam a todos os vizinhos a sua tabela de routing por completo. O nó como tem acesso às tabelas dos vizinhos idêntica ao melhor caminho para cada destino, construindo assim a sua própria tabela de routing

→ RIP:

- mais amigos (=) + simples
- custo (memória) baseado apenas no hop count

- convergência lenta
- não é compatível com endereços de máscara variáveis (VLSM).
- é standard do IETF

- HELLO : • não tem versão standard
 • métrica tem por base o otimismo das ligações
 • tempo de convergência instável
 • não respeita VLSM

- IGRP : • não tem versão standard
 • métrica é a velocidade
 • tempo de convergência é médio, apresentando o melhor desempenho ddo 3

- A rede pode ser tão pesada que não justifique usar protocolos de routing
- Uma rede de média dimensão pode já justificar a complexidade do OSPF para convergir rapidamente.

②. Apresente as áreas funcionais do módulo OSI de gestão de redes, descreva os procedimentos e objetivos para cada uma delas.

1 - Gestão de falhas

- Detecção e localização da falha
- Isolar a falha do resto da rede
- Montar planos alternativos
- Minimizar o impacto do problema
- Reparação ou substituição do equipamento

2 - Gestão da contabilização

- Contabilização do tráfego nas fronteiras da rede
- Detecção de gastos excessivos de um utilizador ou grupo de utilizadores
- Utilização inefficiente dos recursos da rede
- Previsão dos recursos da rede
- Fornecer info. pl. às op. de taxação

3 - Gestão das configurações

- Monitorização
- Controlo p/ melhoria do desempenho da rede
- Verificação do SIA

4 - Gestão do Desempenho

- Proteção da informação
- Controlo de aceso aos recursos
- Gestão centralizada ou distribuída
- Níveis hierárquicos de aceso
- Registo de eventos (logging)
- Análise de logs

5 - Gestão de Segurança

→ Manutenção das versões do SW das inst. de rede
 → Monit. e config. dos sistemas
 → AH, AS config.
 → Atualizações d. SW ou FW
 → Escalonamento das alterações

③ → Já feito no exame modelo

→ SNMPv1 e v2 → sujeitas a packet sniffing da community string (isso inclui a string) → resolvido na v3

→ Ataques de força bruta e de dicionário, p/ adivinhar community string, string de encriptação, chaves de autenticação, etc → não implementam handshake

→ SNMP usado sobre UDP - vulnerável a ataques IP spoofing → resolvido na versão 3

→ community string vir definida como "público" /cpn default.

④. Já feito no exame modelo

MIB RMON → especificação standard de monitorização que possibilita a troca de dados de monitorização da rede entre vários sistemas.

→ Funciona do cliente-servidor onde os dispositivos monitorizados (RMON Probes) têm instalado um software que coleta info e analisa pacotes

→ sondas atuam como servidores, e aplicações de gestão da rede que comunicam com elas atuam como clientes

→ RMON distingue-se pois mesmo utilizando SNMP as sondas têm maior responsabilidade em recolher dados e processar a informação, induzindo o tráfego SNMP.

→ A info recolhida p/ a aplicação de gestão quando pedida, em vez de a enviar automaticamente continuamente.

→ Estes 2 factores resolvem o problema do polling, permitem monitorização constante da rede pelas sondas, NMS e NME, mais do que um NMS → não há problema, sonda auxilia

→ Orientada p/ monitorizar equipamentos e pode precisar do equipamento dedicado p/ monitorizar a rede se querem detalhados segundos.

5.

a) O que entende por sua igual a relevância que lhe se conhece?

SLA → Server Level Agreement - é a formalização do "quality of service" num contrato entre o cliente e o provedor de serviço. Este acordo é importante pois estabelece os requisitos mínimos que devem ser fornecidos. Se o acordo não estiver a ser cumprido, o provedor de serviços deve aplicar uma penalização, mas para isso, é necessário que o cliente monitorize o sistema de maneira a detectar possíveis falhas.

b) Qual a importância da localização dos equipamentos na análise de requisitos?

Já respondida no exame Modulo

c) Diga o que entende por um serviço de aceso à internet com 99,50% de disponibilidade.

Sistema em baixo 43 horas min/ano, não englobando manutenções agendadas.
→ não é aceitável a clientes que necessitem estar sempre operacional
→ pelo uso de triplo redundância: 99,999

d) O que indica o valor do MTBF? Qual a sua relevância?

MTBF → Mean Time between failures - indicação da frequência de falha e a sua medida relativa é a média entre falhas.

A partir deste valor é possível deduzir o grau de fiabilidade de um sistema.

Grupo III

$84 \cdot 155 \cdot 41 \cdot 65 / 30 \rightarrow \text{GW1}$
 $84 \cdot 155 \cdot 41 \cdot 129 / 30 \rightarrow \text{GW2}$
 $84 \cdot 155 \cdot 41 \cdot 193 / 30 \rightarrow \text{GW3}$

$\left. \begin{array}{l} \rightarrow \\ \text{Acesso ao ISP1} \end{array} \right\}$

$195 \cdot 23 \cdot 200 \cdot 160 / 30 \leftarrow \text{Novo ISP2, endereço + baixo é o do NUTZER} \Rightarrow \text{IP interno da rede}$

1. N.º mínimo de redes.

Filiais:

VLAN 1:

10 APs wi-Fi	
4 switches	
+ 1 router	
= 15 est.	
17 endereços $\equiv 1/27$	

VLAN 10:

20 est.	
22 endereços	
\equiv	
1/27	

VLAN 20:

60 est.	
62 endereços	
\equiv	
1/26	

VLAN 30 (servidores locais)

10 est.	
72 endereços	
\equiv	
1/28	

VLAN 40

120 est.	
122 endereços	
\equiv	
1/25	

Sedi:

VLAN 1:

24 APs wi-Fi	
16 switches	
+ 1 router	
= 41 est.	
41 endereços $\equiv 1/25$	

VLAN 10:

96 est.	
98 end.	
\equiv	
1/25	

VLAN 20:

300 est.	
302 end.	
$\equiv 1/23$	

VLAN 30

(serv. locais)	
30 est.	
32 end	
$\equiv 1/27$	

VLAN 40

480 est.	
482 end	
$\equiv 1/23$	

17 endereços
 \equiv
1/26

Cada uma das filiais contém 5 VLANs.

• A VLAN 1 que contém 15 estações. Para ser feito o endereçamento desta VLAN, para além de ser necessário um endereço ao NDU e um de broadcast, também é necessário um endereço 17 endereços, ambiguindo-se, assim, um bloco de 32 endereços ($1/27$). O raciocínio repete-se para cada uma das 4 filiais que têm o mesmo endereço ambiguo.

$$\begin{aligned}
 1/31 &= 2^0 = 1 \\
 1/30 &= 2^1 = 2 \\
 1/29 &= 2^2 = 4 \\
 1/28 &= 2^3 = 8 \\
 1/27 &= 2^4 = 16 \\
 1/26 &= 2^5 = 32 \\
 1/25 &= 2^6 = 64 \\
 1/24 &= 2^7 = 128 \\
 1/23 &= 2^8 = 256 \\
 1/22 &= 2^9 = 512 \\
 1/21 &= 2^{10} = 1024
 \end{aligned}$$

\rightarrow

Número mínimo de endereços: $5 \times 2 + 5 = 15$ end.

Tamanho dos blocos de endereços:

Fícial:

- | | |
|-------------------------|---------|
| VLAN 1 → 32 endereços | → /28 ✓ |
| VLAN 10 → 32 endereços | → /27 ✓ |
| VLAN 20 → 64 endereços | → /26 ✓ |
| VLAN 30 → 16 endereços | → /28 ✓ |
| VLAN 40 → 128 endereços | → /25 ✓ |

Sede:

- | | |
|-------------------------|---------|
| VLAN 1 → 64 endereços | → /26 ✓ |
| VLAN 10 → 128 endereços | → /25 ✓ |
| VLAN 20 → 512 endereços | → /23 ✓ |
| VLAN 30 → 32 endereços | → /27 ✓ |
| VLAN 40 → 512 endereços | → /23 ✓ |

2. Atribuição de Endereços. → de 200.16.120.0 a 200.16.139.255

Sítio	End. Réal.	End. Broadcast	Máscara	VLAN
Sede	200.16.120.0	200.16.125.255	/23 (512)	20
Sede	200.16.126.0	200.16.127.255	/23 (512)	40
Sede	200.16.128.0	200.16.128.127	/25 (128)	10
F1	200.16.128.128	200.16.128.255	/25 (128)	40
F2	200.16.129.0	200.16.129.127	/25 (128)	40
Sede	200.16.129.128	200.16.129.191	/26 (64)	1
F1	200.16.129.192	200.16.129.255	/26 (64)	20
F2	200.16.130.0	200.16.130.63	/26 (64)	20
Sede	200.16.130.64	200.16.130.95	/27 (32)	30
F1	200.16.130.96	200.16.130.127	/27 (32)	1
F2	200.16.130.128	200.16.130.159	/27 (32)	1
F1	200.16.130.160	200.16.130.191	/27 (32)	10
F2	200.16.130.192	200.16.130.223	/27 (32)	10
H1	200.16.130.224	200.16.130.239	/28 (16)	30
F2	200.16.130.240	200.16.130.255	/28 (16)	30

Máscaras:

/23 - 255.255.254.0

/29 - 255.255.255.248

/22:

/24 - 255.255.255.0

/30 - 255.255.255.252

255.255.252.0

/25 - 255.255.128

/26 - 255.255.192

/27 - 255.255.224

/28 - 255.255.240

3.

Horação do trabalho: 9h - 18h = 9 horas

E-MAIL:

- Envia: 20 M byte
- Recebe: 80 M byte

Indídeo recebido:

- 70% ext.
- 30% int.

Indídeo enviado:

- 20% int.
- 80% ext.

WEB:

- 30 M byte interno
- 120 M byte externo

VOIP:

- 4 M byte emmado
- 4 M byte saída
- 80% ext.
- 20% int.

SAP

- 10% util. huias
- 20% util. sede
- 15K byte
- 20 transações diárias

BACKUP:

00:30 às 06:30
3 Gbyte

a) Modelo de fluxos

- e-mail: cliente - servidor
- web : "
- voip : peer-to-peer
- SAP : cliente - servidor
- Backup: cliente - servidor

b) Fronteiras

GW1 - ISP1

ISP1 - GW2

ISP1 - GW3

ISP2 - GW1

c) Fluxos Web, E-MAIL, SAP entre edifícios

Nº utilizadores Sede: $96 + 300 + 480 = 876$

Nº utilizadores Filiais: $20 + 60 + 120 = 200$

E-MAIL :

$$\frac{876 \times 0.13 \times 80M}{9 \times 3600} = 650 \text{ K byte/s}, \text{ recebido sede}$$

$$\frac{200 \times 0.13 \times 80M}{9 \times 3600} = 150 \text{ K byte/s}, \text{ recebido filial}$$

$$\frac{876 \times 0.12 \times 20M}{9 \times 3600} = 110 \text{ K byte/s}, \text{ enviado sede}$$

$$\frac{200 \times 0.12 \times 20M}{9 \times 3600} = 25 \text{ K byte/s}, \text{ enviado filial}$$

Web:

$$\frac{30M \times 876}{9 \times 3600} = 810 \text{ K byte/s}, \text{ rede}$$

$$\frac{30M \times 200}{9 \times 3600} = 185 \text{ K byte/s}, \text{ filial}$$

SAP:

$$\frac{0,1 \times 200 \times 15K \times 20}{9 \times 3600} = 185 \text{ byte/s}, \text{ filial}$$

$$\frac{0,2 \times 876 \times 15K \times 20}{9 \times 3600} = 1,6 \text{ K byte/s}, \text{ rede}$$

d) Décimo airponibilizado

$$\text{Sedu: } 40 \text{ Mb/s} = 5 \text{ M byte/s} \rightarrow$$

$$\begin{array}{r} 810 \text{ K byte/s} \\ 1,6 \text{ K byte/s} \\ 110 \text{ K byte/s} \\ 650 \text{ K byte/s} \\ \hline 1,57 \text{ M byte/s} \end{array}$$

- Rede está sobdimensionada
- dímito SAP é tão baixo que não ateta a dimensão dos fluxos da rede

- Há possibilidade de fazer o backup tanto na hora de expediente c/o durante a noite.

DUVIDAS P/RE

→ Grupo III exame:

- Fronteiras → são as fronteiras situadas nas ligações aos ISPs?
- Utilizadoras não todas as estações discriminadas?
"Cada utilizador tem acesso a um ponto de trânsito e é o um terminal VoIP".
- VLAN dos AP's? conta como uma VLAN?
(IP das endereços)
- VoIP interno ou externo?
- SAP
- Diáscritic débito disponibilizado:

→ MIB privada

→ fornecer informações específicas dos equipamentos como a configuração, as colisões, sendo também possível reiniciar uma ou mais portas de um switch.

→ "O SNMPv3 enquadra-se no modelo de camadas TCP/IP, sobre a camada de transporte TCP"

○ F. UDP??? ← Podem ser as duas!

→ "Uma sonda RMON permite ao agente estender as funções da gestão ao coletar os mapas sonoros na parte da rede em que está inserida"

F ou V? Recolher dados e processar info. da gestão

→ OSPF é simples? complexo.

→ "O BGP4 é um protocolo de routing extensão do tipo distância vector e pode ser usado como um IGP para trocar informações de routing entre roteadores dentro do mesmo AS" V ou F???

↳ quando o BGP é usado neste situação chama-se iBGP
→ Path vector ou distance vector?

→ Soluções para gestão de uma rede caso não suporte SNMP

CMIP
TMN → complexo

GRUPO III (Exame modelo)

- Edifício sede, ligado à Internet em Ethernet 40Mb/s
- Filial, 20 Mb/s.

Filial

- 10 APs para 30 est.

VLAN 10 - serv. admin e gestão
• 20 estações

VLAN 20 - terminais VoIP
• 60 est

VLAN 30 - servidores Web
• 10 est.

VLAN 40 - utilizadores comuns
• 120 est.
(incluindo estações móveis)

E-MAIL:

- Envia 10 Mbyte/dia
- Recebe 25 Mbyte / Dia
- 8 horas
- Tráfego recebido
 - 70% externo
 - 30% interno
- Tráfego enviado
 - 60% interno
 - 40% externo

- Fluxos de e-mail, acesso web, VoIP e SAP: (entra edifícios)

utilizadores :

Filiais : $120 + \cancel{10} + 60 + 20 = 210 =$

Sede : $180 + \cancel{20} + 30 + 96 = 306 =$

→ EMAIL:

$$\frac{25M \times 0,3 \times 210}{8 \times 3600} = 54,7 \text{ Kbytes/s}, \text{ nubindo filial}$$

$$\frac{25M \times 0,3 \times 306}{8 \times 3600} = 136,1 \text{ Kbytes/s}, \text{ nubindo sede}$$

Sede

- 24 APs para 120 estações

→ VLAN 10 - serv. admin e gestão
• 96 est.

→ VLAN 20 - terminais VoIP
• 300 est

→ VLAN 30 - servidores da empresa
• 30 est.

→ VLAN 40 - utilizadores comuns
• 480 (incluindo móveis)

WEB:

- 10Mbyte interno
- 40 Mbyte externo

VOIP:

- 2 Mbyte entrado
- 2 Mbyte saída

SAP:

10% utilizadores filiais
20% " sede
média 15kbyte
dia

BACKUP:

00:00 - 7h
cópia logar 5 Gbyte.

$$\frac{10 \text{ M} \times 0,6 \times 210}{8 \times 3600} = 43,8 \text{ K byte/s}, \text{ enviado filial}$$

$$\frac{10 \text{ M} \times 0,6 \times 906}{8 \times 3600} = 189 \text{ K byte/s}, \text{ enviado sedu}$$

WEB:

$$\frac{10 \text{ M} \times 210}{8 \times 3600} = 73 \text{ K byte/s}, \text{ filial}$$

$$\frac{10 \text{ M} \times 906}{8 \times 3600} = 315 \text{ K byte/s}, \text{ sedu}$$

VoIP:

$$\frac{2 \text{ M} \times 210}{8 \times 3600} = 15 \text{ K byte/s}, \text{ enviado filial}$$

15 K byte/s recebido filial

$$\frac{2 \text{ M} \times 906}{8 \times 3600} = \cancel{15 \text{ K byte/s}} \text{ enviado sedu}$$

~~15 K byte/s~~ recebido sedu

SAP:

10% utilizaciones filiais = 21

20% utilizaciones sedu = 181

$$\frac{21 \times 15 \text{ K} \times 20}{8 \times 3600} = 218,15 \text{ byte/s?}$$

$$\frac{181 \times 15 \text{ K} \times 20}{8 \times 3600} = 1885,42 \text{ byte/s}$$

• Discuta o débito disponibilizado nos access à internet

→ Fone do horário Vok → sedu: 40 Mb/s → 5 M bytes/s

→ Sobredimensionado → filiais: 20 Mbit/s → 2,5 Mbyte/s

→ 26h POK 236 K byte/s 1885,42 byte/s

Thomaz 189 K byte/s

→ concorrente 315 K byte/s

SAP 75 K byte/s

TOTAL: 771,9 K byte/s ???

Prova sem consulta. Duração: 2h00min

Exame de Recurso

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.

 F

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.

um switch é uma maneira

a maneira

 F

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.

pela rotação de destino da rede

 F

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.

UDP

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.

→ Best - Effort
→ Rate Critical

A man) → TEMPO REAL

→ NÃO TEMPO REAL

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

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

O Telnet é uma aplicação que do ponto de vista dos requisitos de acesso pode ser classificada como não sendo de tempo real.

IPv4

8. Um endereço IPv5 de uma rede com uma máscara de 22 bits a "1", permite endereçar no máximo 510 estações ativas na rede.

7682

Prova sem consulta. Duração: 2h00min

Exame de Recurso

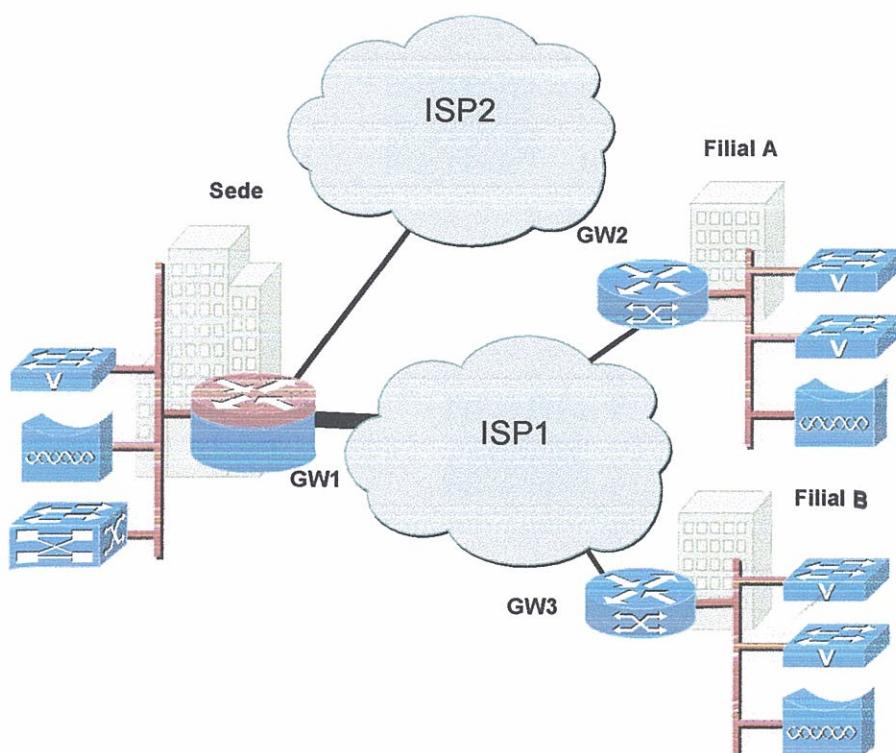
9. O OSPF é o protocolo de routing do tipo *EGP* mais utilizado na Internet devido à sua complexidade, suportar endereços não alinhados à classe, ter rápida convergência e ser uma norma do ICP.

10. O BGP4 é um protocolo de routing exterior do tipo *distance vector* e pode ser usado como um IGP para trocar informação de routing entre routers dentro do mesmo Sistema Autónomo.

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.
- ✓ 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.

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, respectivamente. 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, respectivamente.
- 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:

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

- 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.
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.
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

Grupo I.

1. F. Quando um SWITCH processa uma TRAMA e o endereço MAC de destino é desconhecido (...) a trama é encaminhada ...
2. F. (...) as vezes que faltam necessárias (...) pela estação de destino.
3. F. (...) agente (...)
4. F. UDP
5. F. Best-Effort, Rate-Limiting
6. F. (...) cliente-servidor.
7. F. (...) não sendo de tempo real
8. F. IPv4 (...) 1024.
9. F. (...) IGP (...) TCP/IP (...) devido à superset (...) norma IETF.
10. D. Chama-se iBGP mas é na mesma BGP4.

Grupo II

1. Protocolos de routing são gestados de redes de acesso a uma infraestrutura de rede de média e grande dimensão

= exame exemplo de 2011/2012

Para redes de média e grande dimensão os protocolos baseados em distância-vektor tradicional não são recomendados, sendo então utilizados os protocolos OSPF, EIGRP e IS-IS.

OSPF é um protocolo standard IETF, podendo ser utilizado por qualquer fabricante garantindo heterogeneidade. Este protocolo utiliza o protocolo de routing link-state, sendo dessa forma eficiente, contudo + exigente na capacidade de processamento.

No protocolo de routing link-state os nós anunciam pela rede apenas os seus pacotes link-state para informar os outros sobre o seu estado. Seguidamente os LSP's dos vizinhos vão ser utilizados para construir um módulo global da rede e uma tabela de routing. Os melhores caminhos são calculados pelo algoritmo de Dijkstra. ①

EIGRP é um protocolo que uniu o protocolo de routing de distância vector mas com diferenças face ao original: em vez de enviar a sua tabela de routing por completo apenas envia partes da tabela que os outros nós ainda não conhecem. A vantagem disto é desocupar alguma largura de banda, sendo importante esta modificação no caso de nós de média e grande dimensão.

IS-IS é um protocolo standard OSI semelhante ao OSPF, mas enquanto que OSPF foi desenvolvido para rotear IP, o IS-IS é um protocolo da camada 3 OSI que opera em cima de IP.

OSPF e IS-IS são protocolos standardizados (IETF e OSI, respetivamente). EIGRP é uma evolução do IGRP e foi proprietário da Cisco.

Os três protocolos têm um tempo de convergência baixo ($\approx 10^2$), são complexos.

O OSPF calcula o custo das rotas fazendo a diferença entre a largura de banda de interface e a largura de banda da interface; EIGRP calcula a métrica com base nos atrasos e na largura de banda (velocidade); IS-IS calcula a métrica atribuindo um peso de 10 a cada ligação.

Tanto OSPF como o IS-IS são caracterizados pela divisão da rede em áreas, mas apenas o OSPF precisa que as áreas devem ser todas adjacentes à área 0.

OSPF suporta mais funcionalidades, mas IS-IS é mais escalável e, para os mesmos recursos, consegue suportar mais roteiros na mesma área que o OSPF.

IS-IS é, no entanto, mais complexo.

2. Apresente as áreas funcionais do modelo OSI de gestão de redes, descreva os procedimentos e objetivos para cada uma delas. FCC-DS

1. Gestão de falhas

- Detecção e localização da falha
- Isolar falha do resto da rede
- Reconfigurar ou alterar a rede p/ minimizar o impacto do problema
- Reparar ou substituir equipamento

2. Gestão de contabilização

- Contabilização do tráfego nas montanhas de rede
- Detecção de gastos excessivos de um utilizador ou grupo de utilizadores
- Utilização ineficiente dos recursos da rede
- Previsão dos recursos necessários p/ a evolução da rede
- Fonte de informação para as operações de taxação

3. Gestão de configurações.

- Manutenção das versões de SW dos sistemas de rede
- Manutenção e configuração dos sistemas
- Alterações às configurações
- Atualizações de SW ou HW
- Escalonamento das alterações

4. Gestão do desempenho

- Monitorização
- controlo p/ melhorar o desempenho da rede
- verificação do SLA

5. Gestão de segurança

- Proteção da informação
- controlo de acesso aos recursos ou distribuída
- gestão centralizada de acesso
- Níveis hierárquicos de acesso
- registo de eventos (logging)
- análise de wgs

3. Characterizar SNMPv3, fazendo referência às alterações importantes.

O SNMPv3 mantém o modelo de gestão de redes Internet com quatro componentes, tal como previsto no SNMPv1:

→ Um ou mais nós para gerir, cada um contendo uma entidade SNMP (um Agente) que permite aceder à informação de gestão do nó.

→ Pelo menos uma entidade SNMP de gestão (um Gestor) com uma ou mais aplicações de gestão da rede instaladas

→ Um protocolo de gestão de redes que é utilizado pelo NMS e os agentes para trocar informação de gestão

→ A informação de gestão.

Conceptualmente o SNMPv3 é uma extensão do SNMP na área de Administração e Segurança.

O SNMPv3 contempla adicionalmente quatro áreas de segurança que estavam omissoas no SNMPv2:

- Autenticação: identificação do origem, integridade da mensagem e alguns aspectos de segurança na rede.

- Privacidade: confidencialidade - pacotes para evitar a captura de pontos de autorização - encriptação dos pacotes por rede.

- Autenticação e Controlo de acesso: integridade - assegurada para garantir que um pacote não foi alterado ou a sua ordem modificada ao longo do percurso. Inclui ainda um mecanismo de proteção opcional para envio dos pacotes.

- capacidade de configuração e administração remota por três aspectos adicionais.

4. MIB privada.

A MIB é uma especificação standard de monitorização que disponibiliza a forma de dados de monitorização da rede entre vários sistemas. A MIB específica o elemento de dados (as variáveis a gerir) que um sistema gerível precisa de ter, as operações permitidas em cada variável e qual o seu significado.

A MIB privada é aquela que contém objetos definidos por várias organizações. Fornecendo informações específicas dos equipamentos que estão a ser geridos como a configuração, as correrias, sendo também possível reiniciar e desabilitar uma ou mais portas de um router.

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. Planeamento.

a) SLA

SLA - Service Level Agreement → é a formalização de um contrato entre o cliente e o provedor de serviço. Este acordo é importante pois estabelece os requisitos mínimos que devem ser fornecidos. Se o contrato não estiver a ser cumprido, o provedor de serviços deve sofrer uma penalização, mas para isso, é necessário que o cliente monitorize o sistema de maneira a detectar possíveis falhas.

b) "last foot" e "last mile"

Os problemas last foot e last mile são problemas existentes nos requisitos de equipamentos na área da performance. O "last mile" caracteriza-se como sendo a dificuldade em trazer infra-estrutura, rede e serviços para um campus ou edifício. Trazer até ao dominante do que se encontra na infra-estrutura original, como por exemplo trazer fibra até um condomínio.

O problema "last foot" é a dificuldade em fazer os serviços e a performance da interface de rede do aparelho até às suas aplicações e utilizações. Por exemplo: certa de rede não tem capacidade para aceitar 6Gb, bairramento e processador rápido, diferentes só, diferentes desempenhos.

c) disponibilidade de um serviço de acesso à Internet a 99,50% vs 95%.

→ 99,5% → 43h 48 min/ano em baixo

→ 95% = 432 horas/ano → 18 dias em baixo/ano

→ disponibilidade → quantidade de tempo em que a rede está operacional, n/ contar com a manutenção agendada.

→ não autorizável a clientes que necessitem da rede sempre disponível

→ P1 imo usa-se triple redundância

→ 95% → o que normalmente ocorre aos utilizadores comuns?

d) que tipo de aplicações distinguem na análise os requisitos relativamente ao atraso? Caracterize-as.

• Aplicações em tempo real → telefonemas, videochamadas. Estas aplicações são muito sensíveis ao atraso. Neste tipo de aplicações é preferível perder alguma informação e/ou qualidade do que a informação chegar com um atraso tal que não seja percutível aos utilizadores.

• Aplicações que não são em tempo real → não há grande problema se a informação chegar com algum atraso. É mais importante que a informação chegue completa e n/ erros. Interativas ↙ burst → info chega por picos+tempo bulk → info de grande volume → FTF. Asimétricas → insensíveis ao atraso → e-mail.

④ É necessário medi/monitrar.

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)

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? SLA → Service Level Agreement
- ✓ 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.

User Requirements

- Oportunidades
- Interatividade
- Confiabilidade
- Interface gráfica
- Facilidade de Adaptação
- Segurança
- Orçamento
- Funcionalidades
- Facilidade de Manutenção
- Possibilidades de expansão

Dependências } Requisitos de Rede:

- integrar redes já existentes
- dependências de escalação e de utilização
- localização
- performance
- rede, sistema e serviço de suporte
- inter-operabilidade

Grupo II (40min)

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;
 - Acesso Web – cada utilizador em média acede a 10MB de conteúdos da empresa e 30MB de conteúdos externos;
 - 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;
 - 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.
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)

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 SNMPv3 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 agente estender as funções da gestão ao colecionar 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)

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

1. Requisitos do Utilizador

PI 0A 2(FCS)

Os requisitos do utilizador são aqueles que são dispostos em consona com os utilizadores. Estes requisitos estão directamente relacionados com a performance: amano, fiabilidade e capacidade.

→ Prontidão

→ Interatividade

→ Qualidade de apresentação - questões relacionadas da interface gráfica

→ Adaptabilidade - regras alterações, critérios específicos (tamanho do monitor)

→ Funcionalidade

→ Fiabilidade

→ Custo → orçamento

→ Calendário futuro

→ Suporte

→ Segurança

2. Requisitos específicos da Rede

O principal requisito é o que está quase sempre presente no planeamento das redes é a capacidade de adoptar/criar/expandir algo que já existe - a atualização dos sistemas. É também preciso ter em conta as dependências e as limitações da localização, para evitar, por exemplo, interferências eletrônicas magnéticas. As dependências escalares,

as limitações de performance e as dependências de disponibilidade são também questões importantes neste processo.

3. Componente de Gestão

→ Monitorização

→ Gestão de Protocolos

→ Características a monitorizar

→ Monitorização in-band e out-band < monitor. int. usik

→ Gestão centralizada ou distribuída < monitor. int. usik

→ Performance

4. SLA

Service Level Agreement → é a formalização dos níveis de serviço.

Contrato entre o cliente e o provedor

Este acordo é importante

pois estabelece

os requisitos mínimos que devem ser fornecidos. Se o acordado não estiver a ser cumprido, o prestador de serviços deve aplicar uma penalização, mas para isso, é necessário que o cliente monitore o sistema de maneira a detectar possíveis falhas.

5. Qual a importância da localização dos equipamentos na análise de requisitos

Saber a localização é importante para determinar a utilização entre os utilizadores, as aplicações e a rede. É importante para saber quais componentes do sistema que funcionam são outros.

A localização dos equipamentos é o primeiro passo para determinar características do sistema no que toca a fluxos de tráfego.

6. Diga o que entende por um serviço de acesso à internet com 99,50% de disponibilidade

Não se garante a disponibilidade total do acesso à internet. O sistema podem estar em baixo 43h58 min/ano → quase dois dias, não englobando as manutenções agendadas.

Não é aconselhável a clientes que necessitam que a rede esteja sempre operacional. Para isso deverá comentar a um serviço de triplo redundância: 99,999%.

7. MTTR

MTTR → Mean Time To Repair. É expressa como a média de tempo de reparação de um sistema.

A partir deste valor é possível estimar a manutenção de um sistema.

8. Desempenho de uma rede

- Latência da Banda → capacidade de transpor informação num circuito

- Taxa de Transmissão → quantidade de informação transmitida por unidade de tempo. Informação que de facto conseguimos enviar

- Goodput → quantidade de informação disponível para as aplicações

9. Que tipo de fluxos
Qualas as implicações da previsão de cada um.

- Individual → fluxo associado a uma única sessão aplicacional
- Composto → combinação de vários fluxos (best-effort) individuais que partilham o mesmo caminho, ligação ou nó
- Backbone → é a combinação de vários fluxos compostos quando a rede atinge um certo grau de hierarquia

○ Num projeto de rede, a maioria dos fluxos identificados ou best-effort têm características de baixo desempenho. Só alguns fluxos têm características de alto desempenho ou especificadas.

Fluxos de alto desempenho conduzem o projeto segundo uma perspetiva de serviço.

Fluxos de baixo desempenho conduzem o projeto segundo uma perspetiva de planeamento de capacidade.

10. Modelos de Fluxos

○ Modelos de fluxo são caracterizados essencialmente pelo sua direcionabilidade e pela sua hierarquia.

acimo entre Peer-to-peer: não existe hierarquia, nem dados de acima entre eles equivalentes. exp. Teleconferências

Cliente-Servidor: tem direcionabilidade e hierarquia, pedidos e respostas (a servidores), fluxos assimétricos

en me servidores Computação Coordenada: comunicações entre serviços, e servidores de suporte ou entre servidores e gestores fluxos são considerados críticos

Computação Distribuída: faz tudo q roda a gente

Grupo III:

1. O SNMP é um protocolo de gestão de rede que inclui, unicamente, 3 versões
2. agente
3. N. → pode ser TCP ou UDP
4. V.
5. Apenas no SNMPv3
6. F. O OID é um identificador de um objeto na MIB
← está implícito. → É VERDADEIRO!!
7. F. ~~uma~~ RMON tem a responsabilidade em recolher os dados e processar a informação da gestão (...)
8. V.

Grupo IV

1. Áreas funcionais do modelo OSI de gestão de rede.

1 - Gestão de falhas: engloba a deteção e a monitorização da falha, bem como o seu isolamento, a reparação e substituição do equipamento e a reconfiguração de rede para minimizar o impacto do problema

2 - Gestão da contabilização: contabilização do número excesivo de monitorizações de rede, detecção de gasto excessivo de um utilizador ou grupo de utilizadores, a utilização ineriente dos recursos da rede, a previsão dos recursos necessários para a evolução da rede, rácio de utilização de interfaces de rede, operações de taxação.

3 - Gestão de configurações: manutenção das versões de SW dos sistemas de rede, manutenção e controlo dos sistemas, alteração das config., actualização do HW e do SW, exclusão metade das alterações

4 - Gestão do desempenho: monitorização, controlo e melhoria do desempenho da rede, revisão do SLA

5 - Gestão de segurança: proteção de info., controlo de acesso aos recursos, gestão centralizada de distribuição, nível de loss, nível de eventos, nível hierárquico.

2. JÁ feito no exame exemplo 2013

3. MIB privada de um fabricante
necessidade

Como poderá ser usada pt gestão do respetivo sistema
de rede.

A MIB é uma especificação standard de monitorização que possibilita a troca de dados de monitorização da rede entre vários sistemas.

A MIB define os variáveis para gerir o protocolo TCP/IP. Os objetos geridos são acessíveis via arquivos de informação - a MIB.

A MIB especifica os elementos de dados é um sistema genérico tem que ter, as operações permitidas em cada e qual o significado

A MIB privada fornece informações específicas dos equipamentos q estão a ser geridos como a configuração, as colisões, sendo fb possível reinitializar e desabilitar uma ou + portas de um roteador

MIB privada é aquela q contém objetos definidos por outros organizadores

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

Perguntas do exame de Junho de 2015:

- Comparar RIP, OSPF e BGP4
(não tenho a unteza se era RIP ou IGRP)
- Apresente as áreas funcionais do modelo OSI de gestão de redes. Descreva os procedimentos e objetivos para cada uma delas
- Solução para gestão segura de uma rede, caso haja dispositivos que não suportem SNMPv3
- Explique o que é uma MIB privada, quais as funcionalidades disponibilizadas e vantagens na sua utilização
- Planeamento:
 - Comente quanto à disponibilidade um serviço de acesso à Internet com 99,9%.
(não me lembro de mais)
- Verdadeiros e Falsos:
 - Um endereço IPv5 de uma rede com uma máscara de 22 bits a "1", permite endereçar no máximo 510 estaçõesativas na rede
 - Uma das grandes vantagens do SNMPv3 é permitir fazer a gestão de uma rede local, garantindo a segurança das comunicações entre o sistema de gestão e os agentes residentes nos equipamentos.
(sem unteza:)
 - outband vs inband
 - escalabilidade
 - MTBF
 - Fluxo de dados: origem + destino

Comparar RIP, OSPF e BGP4:

Os protocolos de routing RIP e OSPF dizem respeito a routing interno, enquanto que o protocolo BGP4 diz respeito a routing externo.

O protocolo de routing RIP é baseado no algoritmo de routing distanci-vector, tendo uma complexidade medida e tempo de convergência na ordem dos 90s.

O algoritmo distanci-vector consiste em ter todos os nós de uma rede a enviarem aos nós vizinhos a sua tabela de routing por completo. O nó, como tem acesso às tabelas dos vizinhos idêntica à melhor caminho para cada destino, construindo assim a sua própria tabela de routing.

O RIP é o mais antigo dos protocolos de routing que utiliza distanci-vector, a sua implementação primeira versão baseava-se apenas no hop count, sendo que numa segunda versão já utilizava uma métrica adicional: taxa de transmissão. Este protocolo não é compatível com endereços de máscara variável (VLSM) e é um standard IETF. Por norma é um protocolo de routing que poderá ser usado para redes de pequena dimensão.

O protocolo de routing OSPF, ao contrário do RIP, é baseado no algoritmo link-state. É um standard do IETF, podendo ser utilizado por qualquer fabricante garantindo heterogeneidade.

No algoritmo link-state os nós anunciam pela rede apenas os seus pacotes link-state para informarem os outros nós da rede sobre o seu estado. Seguidamente os LSP's recebidos dos nós vizinhos vão ser utilizados para construir um modelo global da rede e uma tabela de routing. Os melhores caminhos são calculados utilizando o algoritmo de Dijkstra.

Este protocolo, devido à sua complexidade e aos baixos tempos de convergência deverá ser utilizado em redes de média e grande dimensão. O OSPF tem também presente o conceito de área - não obriga a que todos tenham a mesma capacidade de processamento, podendo organizar a rede pelo importância.

estabilidad

No que diz respeito aos protocolos de routing para gestão de rotas de acordo com uma infra-estrutura de grande dimensão, pode ser necessário utilizar protocolos de routing externo como o BGP4. Por exemplo: no caso em que uma empresa tem mais do que uma ligação ao ISP para haver redundância e/ou distribuição de tráfego ou até no caso de uma empresa que tem vários routers para vários ISP's. Resumindo, é necessário usar BGP4 quando existem vários routers de acordo com extensão.

O B&P4 garante a comunicação entre diferentes AS, e tem uma convergência rápido e existem vários critérios para escolher a melhor NOTA.

O algoritmo utilizado no BGP4 é o path vector. Este protocolo cada entrada na tabela de routing contém a rede de destino, o próximo router e o caminho para chegar ao destino. A troca de dados é feita da seguinte forma: os routers da montanha de cada sistema autônomo (ASBR), que participam no routing por path vector, anunciam a sua disponibilidade a outras naes, através de mensagens path vector. Cada router que recebe uma mensagem de path vector tem que verificar se o caminho anunciado está de acordo com a sua política. Se estiver, o ASBR modifica a sua tabela de rotas e modifica também a mensagem, antes de a enviar para o próximo vizinho. Na mensagem modificada envia o seu próprio AS number e substitui a entrada do próximo router com a sua identificação.

Solução para gestão segura de uma rede, caso haja dispositivos que não suportem SNMPv3

Caso haja dispositivos que não suportam SNMPv3 a gestão da rede poderia ser feita através de listas de controlo de acesso, onde só será permitido operações de leitura e não serão ser permitidas operações de escrita, limitando, assim, o dano. A gestão da rede pode também ser feita huma estrutura dedicada para o efecto - gestão outband, normalmente feita através de VPN.

