1 – Numa rede local podem existir Routers, Switches layer 3, Switches layer 2, Access Points e Firewalls. Diga o que caracteriza cada um destes dispositivos, e dê um exemplo de aplicação para cada um deles.

ROUTER- diapositivo que funciona na camada física da rede que permite interligação de sub-redes distintas numa rede. EX. ligação de edifícios dentro de um campus universitário , ligação entre a ESTG e os serviços centrais.**SWITCH LAYER 3** -dlapositivo que funciona com as funções tradicionais de camada 2 para o endereçamento de dados como também incorpora roteamento. EX. segmentação de redes LAN's muito grandes, c/quantidades excessivas de broadcast de modo a evitar a perda de performance e eficiência de LAN.**SWITCH LAYER 2 –** diapositivo que funciona para endereçamento de dados e multiplicar transmições simultâneas de uma sub-rede de modo a não interferir nas outras sub-redes. EX. Segmentação de redes LAN's pequenas com multiplicos domínios de colisão. **ACCESS POINTS –** tecnologia que usa radiofrequência pra a criação de uma WLAN, ou seja, uma sub-rede com mais utilizadores ligados em simultâneo, sem a necessidade de cabos. EX. Distribuição de uma sub-rede WLAN.**FIREWALLS-** tecnologia responsável pela segurança de uma rede, filtrando pacotes indesejados e controlo de todo o trafego de uma rede. EX. Firewall de uma rede com ligação ao exterior.

2 – Explique de forma tão detalhada quanto possível os seguintes conceitos associados às redes sem fios: mecanismos de segurança, canais de comunicação, fontes de interferência, Site Survey e Zona de Fresnel. MECANISMOS DE SEGURANÇA- prevenir intrusões do exterior, erros dos empregados e ataques DoS, autenticação e encriptação**CANIS DE COMUNICAÇÃO – meio usado para transportar uma mensagem do emissor ate ao recepto.FONTES DE INTERFERENCIA –** qualquer fonte que cause interferência na emissão do sinal**SITE SURVEY –** ferramenta para detectar e ultrapassar problemas de performance apos a implementação de uma nova infra-estrutura ou ampliação de uma rede.**ZONA DE FRESNEL –** é a área explicita em torno da linha de vista. A zona de fresnel deve ser calculada e tomada em consideração na fase do projecto.

3 – Estou preocupado com a segurança proporcionada com telefones IP (VoIP), i.e., espionagem, tenho razões para isso? Explique sumariamente o que é o SIP - Session Initiation Protocol. SIP- protocolo baseado em texto para controlar sessões de comunicação, tais como voz e vídeo chamada através de IP. Inclui também vídeo conferenciam streamming de distribuição multimédia, mensagens instantâneas, jogos online entre outros.OU**SIP –** baseado em texto, inspirado em HTML, ratificado pelo IETF em RFC, costuimizavel, centrado na simulação

4 – Numa rede com 2 Switchs (switch A e B) estão ligadas máquinas do departamento de design e outras do departamento administrativo, sabendo que as maquinas utilizadas pelo dep. Design pertencem à VLAN 2 e as outras à VLAN 3 e que os dois switches estão ligados entre si. Diga o que é necessário para que os elementos de cada VLAN comuniquem entre si (embora em switches diferentes). Será possível colocar as maquinas de VLAN´s distintas a comunicar entre si ? Justifique.Não, porque os switchs não se podem comunicar entre si e não é possível colocar 2 vlan distintas a comunicarem-se.**OU**Para que VLAN's comuniquem entre si, terá que ser adicionado um router, ligado ao switch central. Sim, é possível que máquinas distintas comuniquem entre si, sendo apenas necessário que o tráfego passe por um router, apesar de as máquinas estarem na mesma LAN física, o que pode implicar uma degradação de desempenho.

5 – Diga quais as principais categorias de aplicações telemáticas que conhece e dê exemplos de aplicações para cada uma delas (pelo menos 2). Diga quais os requisitos de QoS que definem as necessidades das aplicações. Aplicações Telemáticas Tradicionais : Acesso remoto a ficheiro, acesso remoto de sistemas informáticos, redes sociais, aplicações de acesso á informação **Aplicações Multimédia :** videotelefone, videoconferência, voD (voz sobre pedido), voip(voz sobre IP) **Novas aplicações telemáticas:** telemáticas, supercomputação distribuída, computação GRID. **REQUISITOS**

Debito binário – debito é a medida de quantidade de bits que atravessam um canal de comunicação porunidade de tempo;**Atraso de transito** – parâmetros de qualidade de serviço, essencial para a maioria das aplicaoes continuas ou isócronas

Taxa de erros ou perdas – os erros tem origem em dos factores essências , erros na tansmissao/ recepçao e por congestão na rede

6 – Um sistema de segurança de uma organização pode ser implementado a 5 níveis, utilizando: Firewalls, Anti-Virus, IDS (Intrusion Detection Systems), sistemas de autenticação e VPN's. Explique o papel de cada um deles. FIREWALL- controlo de acesso, autenticação e privacidade, redireccionamento e balanceamento de carga,suporte de redes virtuais privadas, tradução de endereços IP e manutenção de histórico de acesso.**ANTIVIRUS** – proteção contra vírus**IDS** – deteção de intrusões;**SIST. AUTENTICAÇÂO**- garantir a segurança na comunicação**. VPN's** – interligar sub-redes privadas utilizando outras redes.

Descreva os seguintes subsistemas de cablagem, sem esquecer de mencionar os elementos funcionais incluídos em cada um, e diga em que situação poderá ser necessário criar um nível hierárquico adicional para além dos mencionados?a) Backbone de campus - interliga os edifícios dentro de um campus; inclui um distribuidor de campus (CD), os cabos de backbone do campus e as terminações destes. Pode também incluir cablagens, entre distribuidores de edifícios b) Backbone de edifício- interliga o distribuidor de edifício (BD) e os distribuidores de piso (FD); inclui o distribuidor de edifício (BD), os cabos backbone do edifício e as terminações destes. Pode também incluir cablagens entre distribuidores de piso. c) Cablagem horizontal- interliga os distribuidores de piso (FD) e as tomadas de telecomunicações (TO); inclui os distribuidores de piso (FD), a cablagem horizontal e as tomadas de telecomunicações d) Cablagem de área de trabalho- interliga tomadas de telecomunicações (TO) ao equipamento terminal**Preencha a seguinte tabela, com as chaves usadas, de acordo com os tipos de segurança pretendidos, utilizando a encriptação assimétrica, e diga o que entende por: Integridade; Confidencialidade; Autenticação; Funções de não repudiação e Disponibilidade.**

Chaves usadas na codificação	Chaves usadas na descodificação	Tipos de segurança conseguidos
Pública	Privada	Integridade e confidencialidade
Privada	Pública	Autenticação e não repúdio
Pública + Privada	Pública + Privada	Autenticação, não repúdio, integridade e confidencialidade

Integridade: propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (nascimento,manutenção e destruição) ***Confidencialidade***: propriedade que limita o acesso a informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação ***Autenticação*:** certeza de que um objeto (em análise) provém das fontes anunciadas e que não foi alvo de mutações ao longo de um processo ***Funções de não repudiação*:** propriedade que garante a impossibilidade de negar a autoria em relação a uma transação anteriormente feita ***Disponibilidade*:** propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação.

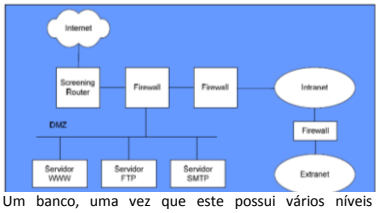
Enumere e caracterize as variantes na norma IEEE 802.11 que conhece, e dê pelo menos três exemplos de aplicação das redes WiFi. Diga quais os mecanismos de segurança que são normalmente implementados num Access Point, e diga para que serve cada um deles.

802.11b: 11Mbps, 2,4 GHz -802.11a: 54Mbps, 5GHz - 802.11g: 54Mbps, 2,4GHz - 802.11n: até 300Mbps, 2,4GHz e 5 GHz - 802.11e: QoS, serviços multimédia - 802.11i: segurança - 802.11h: controlo de potência na gama dos 5GHz - 802.11d: interoperabilidade/compatibilidade entre equipamentos - 802.11f: roaming ***Access Point:*** WEP - Mecanismo de autenticação que funciona através do uso de chaves, ou seja, ao ser definida uma chave, o dispositivo irá funcionar na mesma. Não se indica a utilização do WEP devido ás suas potências falhas de segurança. WPA - É mais seguro que o WEP, baseia-se no protocolo TKIP, que ficou conhecido como WEP2. Aqui a chave é trocada periodicamente, ao contrário do WEP, sendo a sequência definida na configuração da rede. É recomendada. WPA2 - É uma variação do WPA, baseando-se no AES.

Enumere as principais características das fibras ópticas. Diga que tipos de fibras conhece e dê exemplos de utilização habitual de fibras nas SAN´s, LAN´s, MAN´s e WAN´s. O transporte da informação é suportado pela codificação de um feixe de luz; O sinal é gerado por um dispositivo optoeletrónico, normalmente por um díodo LED ou por um emissor lazer; A recuperação do sinal, é feita por um foto-díodo ou por um foto transístor;

As F.O. são constituídas por núcleo central cilíndrico em vidro de silício, rodeado por uma bainha também de silício; Não sofrem interferências electromagnéticas. Fibras Multimodo (Granded-index e step-index) e Monomodo. SAN – ligação de servidores dentro de uma sala WAN – ligação de edifícios numa cidade/país LAN – ligação de servidores entre salas do mesmo edifício MAN – ligação de edifícios dentro da mesma cidade

Desenhe um sistema de Firewall para uma arquitectura de acesso com múltiplas linhas de defesa, para ambiente intranet/extranet, dê o exemplo de uma rede que possa necessitar de um sistema destes. E diga quais as principais funcionalidades e limitações das firewalls



Um banco, uma vez que este possui vários níveis (diferentes entre si) de defesas, diminuindo assim a tentativa de intrusão por parte exterior, nomeadamente de hackers. **Limitações:** não detecta intrusos que estejam dentro da rede; não protege contra conexões que não passem por ele; não oferece proteção contra novas ameaças; pode constituir ponto de degradação da rede; não protege contra vírus e worms. **Funcionalidades**: controlo de acesso; autenticação, privacidade; principal centro de decisões de segurança; tradução de endereços, NAT; manutenção de históricos de acesso; pode servir como plataforma VPN (redes virtuais privadas).

Indique para que servem, e com o funcionam as VPN's. Dê dois exemplos concretos de aplicação

Para que servem: ampliar a area de conectividade; aumentar a segurança; reduzir custos operacionais; aumentar a produtividade; simplificar a tecnologia da rede; promover suporte a utilizadores remotos externos

Como funcionam: A VPN estabelece uma rede privada de modo que os dados podem ser enviados de maneira segura entre esses dois locais. Esse enlace direto ou "túnel" possibilita que todas as aplicações localizadas na rede principal fiquem acessíveis a partir do local remoto.

Exemplos concretos de aplicação: Acesso remoto para funcionários de uma empresa; Extranet para parceiros comerciais.

Diga o que entende por: Integridade; Confidencialidade; Autenticação; Funções de não repudiação e Disponibilidade. Integridade: propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (nascimento,manutenção e destruição) **Confidencialidade**: propriedade que limita o acesso a informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação **Autenticação:** certeza de que um objeto (em análise) provém das fontes anunciadas e que não foi alvo de mutações ao longo de um processo **Funções de não repudiação**: propriedade que garante a impossibilidade de negar a autoria em relação a uma transação anteriormente feita **Disponibilidade**: propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação