

- ➔ MPLS L3 VPN – Fornece capacidade de desenvolver e administrar serviços de camada 3 a clientes de negócio;
- ➔ MPLS L2 VPN – Conectividade entre clientes ao nível de redes de camada 2;
- ➔ MPLS-TE – Faz uso das capacidades de forwarding do MPLS e implementa TE fornecendo mais capacidades de roteamento a redes MPLS.

Rede Overlay – Rede construída com base numa já existente. Pode consistir em software de encaminhamento instalado em sites desejados, ligados por túneis ou links diretos (exemplo disso as P2P e as CDN's).

CDN (Content Distribution Network) – Uma CDN é uma rede de servidores que fornece conteúdo aos utilizadores com base num servidor original. O objetivo é fornecer informação de forma rápida, e com alto desempenho, sem ter de sobrecarregar o servidor original (permitindo maior largura de banda e disponibilidade no acesso ao conteúdo). Os CDN fornecem grande parte do conteúdo online hoje em dia (ficheiros descarregáveis, aplicações, ficheiros web, etc). Um operador CDN é pago pelos servidores originais para fornecerem conteúdo, e em contra partida, um CDN paga ISP's e operadores de rede por estarem alojados no servidor original.

P2P (Peer-to-Peer) – Rede onde cada computador presente nela pode agir como cliente ou servidor para outros computadores na rede, permitindo partilha de dados (audio, video, informação, etc). Neste modo não há uma infraestrutura central, há uma descentralização da rede. Um nó na rede (computador) que pretender ser servidor vai ter de fornecer uma parte das suas capacidades (energia de processamento, espaço de disco, largura de banda) para os outros nós na rede poderem aceder-lhe. Não há uma monitorização central de um servidor. Existe em três modos de disponibilização da informação:

- **Centralizada** – Existe um servidor central para upload e download de ficheiros (Google). Tem como grandes vantagens o rápido tempo de resposta e pesquisas eficientes, mas como desvantagens a estrutura (em caso de falha não há como aceder), existência de administração e custo;
- **Distribuída/Flooding** – Qualquer nó na rede pode atuar como servidor para upload/download (Gnutella). Tem como grandes vantagens o bom tempo de resposta e escalabilidade, não existência de uma estrutura e administração, em caso de falha podemos tentar outros nós. Apresenta como fraquezas o elevado tráfego feito, não realização de buscas estruturadas e rápidas;
- **Híbrida** – Misto de centralizada e distribuída, para redundância. Tem como vantagens a não existência de um ponto de falha central, pesquisas eficientes e como desvantagens, maior complexidade de nós.

As redes P2P podem ser construídas de duas formas:

- **Desestruturadas** – Construídas quando a rede overlay é estabelecida arbitrariamente. Quando um par quer encontrar um pedaço específico de informação, tem de fazer flood à rede;
- **Estruturadas** – Implementam os protocolos adequados para assegurar quem qualquer par na rede é capaz de encaminhar o cliente para um par com os ficheiros pretendidos, mesmo que o ficheiro seja raro (DHT – Distribution Hash Table).

RTP (Real Time Transport Protocol) – Divide-se em dois protocolos que operam sobre UDP:

- **RTP** – Responsável pela emissão de dados multimédia numa rede IP. Uma sessão RTP consiste num endereço IP e num par de portas para RTP e RTCP. Existem ainda sessões "light" em que não há controlo sobre os grupos de participantes (adequado a multicast). Existem dois tipos de entidades RTP:
 - **Translators** – Modificam o formato da informação, não alterando o SSRC ou timestamp (multicast -> unicast);
 - **Mixers** – Geram uma única saída com base em várias entradas CSRC. O SSRC da saída vai ser o do mixer.

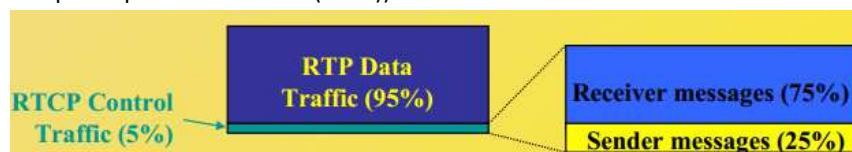
Um cabeçalho RTP contempla alguns atributos importantes:

- **CSRC Count** – Número de identificadores CSRC (usado no modo mixer);
- **Marker** – Anuncia limites de frames;
- **Payload Type** – Campo de 7 bits que define o tipo de codificação para a aplicação;
- **SSRC (Synchronization Source Identifier)** – Identifica a fonte de sincronização (numero aleatório gerado pelo RTP). Todos os pacotes da mesma fonte têm um mesmo SSRC, tipos diferentes (audio, video) têm SSRC diferentes;
- **CSRC (Contributing Source Identifier)** – Lista de fontes que contribuíram para o payload do pacote (usando quando um mixer combina vários pacotes);

- **Timestamp** – Campo de 32 bits que indica o tempo de quando foi recebido o primeiro byte do primeiro pacote (para audio, o timestamp aumenta 1 por cada periodo). Isto vai permitir a quem receber o pacote reproduzi-lo nos intervalos de tempo correctos, sincronizando devidamente audio e video;
- **Sequence Number** – Campo de 16 bits, usado pelo receptor para restaurar o pacote recebido na devida ordem, possibilitando detetar erros. Começa com um número aleatório, e vai ser incrementando a cada pacote RTP enviado.

O RTP não consegue reservar recursos nem garantir QoS, não suporta controlo de congestão, e dessa forma precisa de trabalhar com outros protocolos e redes para isso (RSVP, redes ATM)

- **RTCP** – É como a irmã do RTP, responsável pelo controlo da emissão de dados do RTP, avaliando a qualidade da transmissão e QoS, sincronizando multiplas emissões, permitindo verificar se a transmissão sofreu mudanças de comportamento e informando constantemente tanto o emissor como o receptor do estado da transmissão. É essencial para multicast, uma vez que ao enviar para vários é necessário um maior controlo e monitorização da transmissão. O RTCP está associado a uma porta, e na porta par imediatamente a seguir vai ocorrer a transmissão RTP. O RTCP usa apenas 5% da largura de banda da sessão. Desses 5%, 25% é para os emissores, e 75% é para os receptores. Outra característica de escalabilidade consiste em enviar relatórios com um atraso variável (diferentes periodos, definidos com base no numero de participantes na sessão (SSRC)).



- Os pacotes RTCP dividem-se em vários tipos:
 - **SR (Sender Report)** – Envio de estatísticas para o emissor;
 - **RR (Receiver Report)** – Envio de estatísticas para o receptor;
 - **SDES (Source Description)** – CNAME, nome, email, etc;
 - **BYE** – Deixar a sessão (SSRC de quem deixa, e razão);
 - **APP** – Especifico, conforme a aplicação.

ALF (Application Level Framing) – Controla a forma como a informação é colocada nos pacotes. A aplicação vai dividir a informação em pequenos blocos chamados ADU's (Application Data Units) que podem ser processados numa ordem qualquer. Aparece na estrutura hierárquica do RTP. O ALF precisa sempre de conhecer o canal por onde vai enviar a informação, porque a codificação é sempre sensível na rede.

H.261 – Codificação video, que usa um mecanismo de predição de imagem, considerando diferentes codificações conforme o tempo (frame N é diferente de frame N-1). Se ocorrer perda de pacotes, ele sincroniza com o proximo bloco. Ele vai comparar um frame referência com um frame de entrada, subtrai, e codifica o resultado.

RTSP (Real Time Streaming Protocol) – Protocolo cliente-servidor que permite o control de uma stream (rewind, pause, forward, play, etc). É diferente do RTP visto que não define como o formato é encapsulado para streaming. Não impõe mecanismos de tráfego (UDP ou TCP) e não descreve como o audio/video é reproduzido. Apenas se limita a controla-lo.

VoIP – Conjunto de protocolos e equipamentos que permitem codificação, transporte e encaminhamento de chamadas audio (multimedia) através de redes IP. As streams de audio são codificadas e encapsuladas em pacotes IP para serem transportados na rede (é necessário a devida sinalização (processos de interação entre nós de uma rede por forma a controlar chamadas)). VoIP tem como grande vantagem os custos reduzidos (não é preciso pagar) e o facto de que não depende de operadores. Como a qualidade é semelhante à de telefones, existem várias companhias a investir nestes serviços para diversas aplicações.

SIP (Session Initiation Protocol) – Protocolo independente do protocolo de comunicação (UDP (embora trabalhe preferencialmente por este), TCP), responsável pelo inicio de uma sessão P2P multimédia. É diferente do RTP, porque o SIP inicia a sessão, o RTP realiza a troca de informação. Permite criar, modificar e terminar sessões multimedia entre dois ou mais participantes. Tem funcionalidades que permitem saber: localização (por email) e disponibilidade do cliente, capacidades do cliente, negociação de parametros para participação numa sessão, e implementa ainda alguns mecanismos de segurança (prevenção de DoS, autenticação de cliente, integridade e privacidade de mensagens). O SIP baseia-se nos seguintes componentes:

- **UAC (User Agent Client)** – Aplicação que começa a chamada;

- **UAS (User Agent Server)** – Aplicação que aceita, redireciona ou rejeita a chamada;
- **Servidor de Redirecionamento** – Redireciona as chamadas para outros endereços do UA;
- **Servidor Proxy** – Entidade intermédia que se comporta como servidor e cliente, controla a chamada, obtém o endereço do cliente, pode redirecionar;
- **REGISTRAR** – Regista a localização do utilizador (User Agent). Permite o mapeamento de endereços de utilizadores e os respetivos endereços UA, guardados numa base de dados. Para aceder a ela usa-se o servidor proxy ou o de redirecionamento.
- **User Agent** – UAC + UAS, são as pontas da sessão, terminam e iniciam a chamada.
- **URI (Uniform Resource Identifier)** – Traduzido pelo servidor proxy, para o endereço do UA do utilizador. Um mesmo utilizador pode ter vários endereços UA

As mensagens SIP dividem-se nos seguintes métodos:

- **REGISTER** – Registrar um UA no serviço de localização;
- **INVITE** – Estabelecer ou alterar os parâmetros de uma sessão;
- **200 OK** – Sinalizações de confirmação por parte do emissor;
- **ACK** – Confirmar a receção da resposta a um INVITE;
- **CANCEL** – Terminar um pedido de sessão pendente;
- **BYE** – Terminar uma sessão;
- **OPTIONS** – Interrogar um utilizador sobre as suas capacidades.

O servidor Proxy ou um UA pode pedir a quem inicie a chamada que mostre autenticação. O mecanismo RFC3261 fornece autenticação e proteção.

SDP (Session Description Protocol) – Protocolo que descreve os parâmetros para se iniciar uma sessão multimedia (SIP), como o anúncio de uma sessão, pedidos para join, etc. Tal como o SIP não transfere informação, mas entra no papel de negociação de uma sessão.

H.323 – Protocolo para comunicações multimédia via UDP. Define controlo e sinalização de uma chamada, transporte e controlo multimédia, controlo da largura de banda de uma comunicação, tipos de codecs usados, ou seja, define tudo! Tem cinco componentes essenciais:

- **User Agent** – Agentes envolvidos na sessão;
- **Gatekeeper** – Principal ponto de monitorização da rede. Faz a tradução de endereços (IP-telefone), controla o acesso da rede aos recursos disponíveis, monitoriza as chamadas e controla a largura de banda, bem como controla todos os endpoints de uma rede (devem estar todos registados no gatekeeper). Contudo, é opcional, se não existir, não há controlo da comunicação;
- **MCU (Multipoint Control Unit)** – Suportam as funcionalidades necessárias para vários terminais e gateways participarem numa sessão.
- **Gateway** – Permitem a comunicação entre várias redes H.323.

O processo de início de uma comunicação H.323 requer os seguintes passos: obter a permissão do gatekeeper (RAS Admission Request); procurar o endereço do utilizador a usar (RAS Address Resolution); fazer a chamada (Q.931); perguntar o tipo de linguagem/codec a usar; esperar pela comunicação com as capacidades do utilizador; informar que linguagem vai ser usada na comunicação; começar a conversa; terminar conversa com BYE; desconectar; informar o gatekeeper que a chamada terminou. O H.323 usa o Q.931 para sinalizações de chamada (iniciar, controlar e terminar), o H.245 para criação dos canais de comunicação e troca de capacidades.

Comunicação PSTN (Public Switched Telephone Network) – VoIP - A PSTN comunica com VoIP (em termos de sinalização usando um softswitch (interliga chamadas telefónicas de uma linha para outra através da Internet, através de software num computador) para fazer a tradução de endereços de SS7 para SIP). Os dados passam de DS0 para RTP. Basicamente é atribuído um número de telefone na rede pública normal ao dispositivo VOIP e um IP ao telefone quando este comunica com o cliente VoIP. E estes enviam a comunicação para este tradutor, que reencaminha a informação no formato correcto.

Redes Wireless – Desenhadas de acordo com o número de utilizadores e área de cobertura:

- **PAN (Personal)** – Muito limitadas, mas custo e informação têm custos baixos (Bluetooth);

- **LAN (Local)** – IEEE 802.11;
- **WAN (Regional)** – GSM, UMTS;
- **Worldwide (Satellite)** – De alto custo (Iridium);

Sistemas de telefonia celular:

- **1G** – Sistemas analógicos (450-900 MHz), sinalização feita por FSK e a troca de informação por FDMA;
- **2G** – Sistemas digitais (900, 1800, 1900 MHz), troca de informação por TDMA/CDMA;
- **2.5G** – Extensão para troca de pacotes, modo Digital: GSM -> GPRS, modo Analógico: AMPS -> CDPD;
- **3G** – Redes para aplicações de dados, taxas elevadas, acesso à Internet, troca de informação por TDMA/CDMA.

GSM (Global System for Mobile Communications) – Controla três tipos de serviços: serviços de suporte (para comunicar com ISDN e PSDN), serviços de telefone (transmissões de voz de alta qualidade, mensagens até 160 caracteres e serviços de fax. Estes serviços foram mais tarde reforçados com a WAP (Wireless Application Protocol) e o GPRS (General Packet Radio Service), permitindo enviar pacotes ainda maiores. A rede GSM é repartida em três componentes principais:

- **BST (Base Station Subsystem)** – Composto por vários BTC's (Base Transceiver Stations), que tratam de toda a recepção e comunicação para os nossos telemóveis. Estes BTC's suportam vários alcances e capacidades, e juntos formam uma estrutura que cobrem áreas grandes e espalhadas em zonas rurais, pequenas e apertadas em áreas urbanas. Os BTC's vão comunicar com uma BSC, que vai controlar a possibilidade de nos deslocarmos entre várias áreas sem que a chamada venha abaixo (handover), possibilitar o envio de sinais para telefones específicos responderem (paging), bem como a comunicação com o MSC.
- **MSC (Mobile Switching Centre)** – É a espinha dorsal do GSM. Permite controlar a handover entre vários BSC's e implementa e controla também serviços adicionais sobre os componentes ditos acima. Nesta componente temos ainda o HLR (Home Location Register) e o VLR (Visitor Location Register), que funcionam em conjunto como uma base de dados de informação dos utilizadores na rede e imediações. O HLR guarda os registos permanentemente, e o VLR guarda-os dinamicamente, permitindo poupança de tempo no acesso ao HLR.
- **Operation Subsystem** – Contem um centro de autenticação (AUC) e equipamento de identificação de registos (EIR), usados para segurança.

Canais Lógicos – Canal de comunicação entre duas camadas numa rede, usado para transferência de informação. Os canais lógicos estão distribuídos por canais físicos. Um canal físico consiste num espaço de tempo definido, num canal específico. Assim o canal físico trata do espaço de tempo, e o canal lógico trata da informação transportada pelo canal físico. Temos canais de transmissão a full rate (TCH) e a half-rate (TCH/H). Um canal lógico comporta-se também como um canal de sinalização, sincronizando a rede móvel com o telemóvel, e informando-a de pormenores do telemóvel e canais. Existem vários tipos de canais lógicos:

- **BCH (Broadcast Channel)** – Difunde informação por forma a descrever a actual estrutura do canal de controlo;
- **CCH (Common Control Channel)** – Tratar dos pedidos, respostas, localizações, etc;
- **D/ACCH (Dedicated/Associated Control Channel)** – Troca de sinalizações durante a chamada, atualizações de localização.

A evolução do GSM permitiu a criação de:

- **HSCSD (High Speed Circuit-Switched Data)** – Baseado em rápidas trocas de circuito, criando velocidades 4 a 6 vezes mais rápidas que no GSM (até 43.2kbps). Isto é conseguido com base no uso de vários espaços de tempo,
- **GPRS (General Packet Radio Service)** – É orientado à conexão. Ao contrário do HSCSD, o GPRS não se baseia no tempo de comunicação, mas sim na quantidade de informação transmitida, e não tem uma QoS garantida durante a conexão, esta varia de acordo com o número de utilizadores. Isto vai permitir transferências mais rápidas, na ordem dos 150kbps, permitindo a criação de aplicações de rede. A transmissão GPRS é feita por tunel, e controlada por GTP. Permite sinalização e métodos de cifra, garantindo mais segurança. Em termos de arquitetura, existem dois módulos novos: um SGSN (Serving GPRS Service Node), responsável pelo encaminhamento de pacotes de e para a área de serviço do SGSN para todos os clientes nessa área, e um GGSN (Gateway GPRS Service Node), que funciona como gateway entre a rede GPRS e a rede pública, podendo conectar ainda com outras redes GPRS por forma a facilitar o encaminhamento. Por forma a se registar numa rede GPRS, um utilizador faz um GPRS attach (ligação à rede GPRS), ativando de seguida um contexto PDP (Packet Data Protocol), alocando um PDP no SGSN (vai autenticar o utilizador e

do equipamento) e no GGSN para esse utilizador. O utilizador vai receber um pacote PDP com especificações da sessão. Quando deixa a rede, é efetuado um GPRS detach.

- **EDGE (Enhanced Data Rates for GSM Evolution)** – Rede 3G de baixo custo tem a mesma estrutura do GPRS aumentando a taxa de transferência (144kbps até 470kbps);
- **UMTS (Universal Mobile Telecommunication System)** – Rede 3G que faz uso do W-CDMA (Wideband Code Division Multiple Access) para oferecer boas taxas de transferências

Encaminhamento triangular – Método de transmissão de dados que envia um pacote para um proxy antes de o enviar para o destinatário. Um pacote pode ser enviado diretamente de um host A para outro host B diretamente, enquanto que ao ser enviado do host B para o host A, toma outro caminho antes de chegar ao host A. Isto pode acontecer devido à existência por exemplo de uma firewall.

Gestão de rede – Implementar, integrar e coordenar recursos (hardware, software, pessoas) por forma a se conseguir planear, operar, controlar, analisar, testar, avaliar, desenhar e expandir um sistema por forma a se garantirem objetivos com um custo e recursos razoáveis.

Gestão de redes perspetiva comercial – Os problemas têm de ser resolvidos rapidamente, a rede tem de ser simples, as pessoas não necessitam de realizar regularmente as mesmas tarefas e permite um melhor aproveitamento dos recursos. Por isto tudo é necessário uma gestão de redes, que vai permitir menores custos, maior eficiência, melhor serviço.

SNMP (Simple Network Management Protocol) – Protocolo cliente-servidor para gerir dispositivos numa rede. Tem sempre 1 ou mais administradores a gerirem clientes. Os clientes vão reportando informação para os administradores por polling. Faz um bom uso dos agentes da rede, é simples de implementar, robusto e extensível. No entanto é muito simples, não é escalável, o uso de polling cria muito overhead, tem muitas especificações.

Sistema Baseado em Políticas – Dividido em:

- **Ferramentas de gestão de políticas** – Usado para criar as regras de políticas;
- **Repositório de políticas** – Guarda as regras de políticas;
- **Consumidores de políticas** – PDP (Policy Decision Points) tomam decisões e transfere as regras de políticas para os alvos de políticas (por COPS);
- **Alvos de políticas** – PEP (Policy Enforcement Points) são elementos que vão ser afetados pelas regras de políticas.

COPS (Common Open Policy Service) – Protocolo baseado em TCP (cliente-servidor) usado na interação entre um PDP e um PEP. Mantém uma sincronização entre os dois, recuperando de falhas e enviando KEEP-ALIVES. PDP envia notificações para o PEP, PDP recebe as políticas por SNMP ou LDAP. Suporta dois tipos de clientes: Outsourcing (RSVP), ou seja o PEP comunica com o PDP quando for tomada uma decisão, ou Configuration Requests (DiffServ), quando o PDP configura o PEP com informações de equipamento específica, fazendo uso de um PIB (Policy Information Base) para manter as informações de provisão.

CMIS (Content Management Interoperability Services) – Controla sistemas de gestão diversos e repositórios usando protocolos web. É orientado a objetos.

CMIP (Common Management Information Protocol) – Fornece uma implementação para os serviços definidos pelo CMIS, permitindo a comunicação entre aplicações de controlo e agentes de controlo. Trata a informação na forma de objetos, possibilitando alterações sobre eles. O CMIP trata desses objetos através de GDMOs (Guideline for the Definition of Managed Objects). As instâncias do GDMOs são MIB. Não apresenta comportamentos muito bem definidos, promovendo a flexibilidade. No entanto é complexo (envolve várias camadas), há poucos sistemas que se baseiam em CMIP, poucos agentes CMIP, e normalmente é rejeitado na Internet.

Modelos de gestão:

- **Anárquico** –
- **Reativo** –
- **Proativo** –
- **Orientado a serviços** –
- **Aumento de negócios** –

TMN (Telecommunications Management Network) – Larga rede que permite o control de redes de telecomunicações e serviços. A sua estrutura, protocolos e interfaces permite a ligação entre vários sistemas operativos e equipamentos de telecomunicação. O seu modelo de estrutura divide-se em:

- **NEL (Network Element Layer)** – Camada base;
- **EML (Element Management Layer);**
- **NML (Network Management Layer);**
- **SML (Service Management Layer);**
- **BML (Business Management Layer)** – Camada topo;

Estas camadas podem ser combinadas com as gestões seguintes, formando a matriz TMN:

- **Gestão de Contas** – Deteta o uso de recursos e a sua disponibilização para ficarem disponíveis para utilizadores. Garante o controlo de acesso por parte do utilizador;
- **Gestão de Segurança** – Mecanismos de controlo de acesso à informação da rede. Controlo de pontos de acesso, criação de logs e alarmes por razões de segurança;
- **Gestão de Configurações** – Configuração de elementos críticos de controlo da rede. Pode identificar, agir, juntar informação, fornecer comandos aos sistemas para iniciarem, manter ou terminar conexões;
- **Gestão de Desempenho - Mede** o desempenho da rede (hardware e software) através de medições de percentagem de uso, taxas de erros, tempo de resposta, etc.
- **Gestão de Falhas** – Pode ser feita por:
 - Monitorização à base de notificações;
 - Implementar RMON (cria valores de tráfego e desempenho);
 - Usar filtros para eventos e alertas próximos dos elementos controlados (menos tráfego e complexidade);
 - Procura da base do erro;
 - Implementação de mecanismos de falhas (diminui a redundância).