Limitações de ambientes móveis:

- ➔ **Rede Móvel**
  - Heterogeneidade de multiplas redes indepentendetes
  - Queda de ligação frequente
  - Largura de Banda Limitada
- ➔ **Mobilidade**
  - Não existe noção de mobilidade pelos sistemas e aplicações
  - Problemas de manutenção de rotas nos routers
- ➔ **Dispositivo Móvel**
  - Pequeno tempo de vida da bateria
  - Capacidades limitadas

Internet hierárquica – Existe um backbone ISP que fornece serviço a ISPs cada vez mais pequenos, e estes eventualmente fornecem serviços aos utilizadores. No entanto a hierarquia não é respeitada.

Comutação de pacotes – Pacotes são encaminhados através de ligações partilhadas entre nós da rede. Optimiza o uso da largura de banda e minimiza a latência (tempo que pacote demora a atravessar a rede), aumentando a robustez da comunicação.

Comutação de circuitos – Pacotes são encaminhados através de uma ligação dedicada entre nós da rede, fazendo uso do máximo de largura de banda possivel.

Serviços de transporte de dados: Devem contemplar os seguintes critérios:

- ➔ **Perda de Pacotes**
  - Algumas aplicações estão susceptiveis a perda de dados (audio/video), outras não (transferência de ficheiros);
- ➔ **Largura de Banda**
  - Algumas aplicações requerem certa largura de banda para serem efectivas (multimedia), outras usam a que houver (aplicações elásticas, email, tranferência de ficheiros);
- ➔ **Temporização**
  - Algumas aplicações requerem baixos atrasos para serem efectivas (jogos), outras não têm limites (não têm requisitos de tempo real);
  - **Aplicações Elásticas –** Usam a largura de banda que conseguirem (transferência de dados por HTTP ou FTP);
  - **Aplicações Inelásticas –** Requerem determinada largura de banda (telefones, jogos);

Estrutura de uma rede – Os router fronteira definem:

- **Sistemas Autónomos (AS) –** O encaminhamento é intra-dominio, têm politicas internas próprias, e usam sobretudo os protocolos RIP e OSPF. Normalmente administrado por apenas uma entidade;
- **Interligação de ASs –** O encaminhamento é inter-dominio, e usam sobretudo o protocolo BGP;

Arquitetura da Rede

- ➔ **LAN (Local) vs WAN (Wide) vs MAN (Metropolitan)**
  - LAN opera numa área geográfica restrita, dentro de uma rede de pequeno-média dimensão permitindo partilha de dados (servidores, impressoras, segurança) entre computadores e equipamentos. Normalmente implementadas com Ethernet e administrada por uma única entidade;
  - WAN não tem limites geográficos, liga nós sob dominios administrativos distintos;
  - MAN opera numa área geográfica para além da LAN mas restrita a uma comunidade (cidade por ex.). Apresenta assim desempenho de LAN, mas consegue operar sob dominios administrativos da WAN, ou seja, permite interligação entre locais de uma mesma organização, e permite ao mesmo tempo ligar as organizações.
- ➔ **Acesso**
  - Estabelece ligação entre o Core e o equipamento terminal;

- Tem funções de distribuição e agregação de informação;
- Vulnerável a ataques de segurança e avarias;

➔ **Core**

- Grande capacidade de transporte;
- Suporte para vários tipos de tráfego (QoS);
- Elevada tolerância a falhas.

Tecnologias de Acesso

➔ **Dial Up**

- Existência de um modem para a banda da voz que converte os dados em sinais eléctricos na banda dos 200Hz aos 3,4 Khz. No entanto é impossivel usar o serviço de voz enquanto estivermos a usar o de dados

➔ **xDSL (Digital Subscriber Line)**

- Meio físico fixo de cobre, utilizado para serviço de voz fixo, reutilizado para acessos de banda larga e serviços de dados
- Dedicado desde o operador até ao cliente, fazendo uso da tecnologia de transporte ATM
- Possibilidade de atribuição de um endereço público permanente
- Tem como principais elementos:
  - Modem ADSL ou ATU-R (ADSL Termination Unit – Remote)para acesso à rede por parte do cliente
  - DSLAM (DSL Access Multiplexer) que permite a concentração de dados de multiplas linhas DSL para ligação à rede Core (devido às limitações de banda máxima e perdas evoluiu-se depois para o DSLAM IP com QoS e Multicast IP)
  - BBRAS (Broadband Remote Access Server), que termina ligações para o cliente e para a rede (usado para routing e QoS)
  - Servidor AAA (Authentication, Authorization and Accounting), faz o que os AAA dizem
- Tem vários tipos:
  - ADSL (Asymetric, 24Mpbs downstream, 3.3Mbps upstream), SDSL (Symmetrical, >0.768 Mbps em cada direção), HDSL (High bit-rate, 2 Mbps em cada direção), VDSL (Very High Speed, 51.84 Mbps downstream, 16Mbps upstream). Quando o ADSL não chega a todos os clientes, instalam-se mini e micro DSLAMs (DSLAM com menor capacidade).
- Faz uso de vários protocolos
  - PPP (Point-to-Point Protocol), usado nos acessos Dial-Up ao ISP, possibilita a identificação do utilizador, com autenticação (CHAP e PAP);
  - PPPoE (over Ethernet), usados nos ISPs ADSL, permite controlar o acesso de uma forma já conhecida pelos utilizadores, ao nivel do utilizador e não local. É possivel escolher o ISP

➔ **CATV (Community Access Television)**

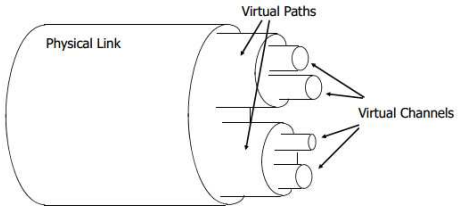
- Rede uni-direcional para difusão de canais de televisão (evoluiu para bidirecional para transporte de dados)
- Composta por cabo coaxial e óptico (HFC – Hybrid Fiber Coaxial), todos os terminais na rede recebem o mesmo sinal, sendo necessário depois mecanismos de segurança para privacidade
- DOCSIS (Data-Over-Cable Service Interface Specification), faz uso dos canais de TV para transporte de tráfego digital (dados, voz e video), com uma mesma banda para todos os utilizadores
- Tem como principais elementos:
  - Modem por cabo ou router por cabo ou set-up-box para o cliente
  - CMTS (Cable Modem Termination System) para o operador, com capacidade para gestão de pilhas IP, atribuição de recursos MAC e adaptação de meios físicos e lógicos

➔ **WLAN (Wireless LAN)**

- Acesso sem fios a serviços de Internet, usando mecanismos e protocolos de rede local
- Temo como principais vantagens a mobilidade, disponibilidade, baixo custo de instalação da estrutura de suporte e facilidade de instalação e utilização do terminal, e a capacidade de existência em locais públicos (PWLAN, que fazem uso de um AZR (Access Zone Router) para routing IP entre vários terminais, com a gestão de endereços IP a cargo de um servidor DHCP)
- Capacidade para um unico AP de suportar vários SSID, podendo cada um deles ter o seu próprio processo de autenticação e politicas de QoS

➔ **ATM (Asynchronous Transfer Mode)**

- Mecanismo orientado à conexão (necessidade de estabelecer uma comunicação primeiro), baseada na comutação de células de dados (53 bytes) que transportam pacotes com determinado tamanho
- Uma rede ATM é hierárquica, com equipamentos de utilizadores a ligarem-se por UNI (User-Network-Interface) e ligações entre redes feita por NNI (Network-Network Interface)
- Permite altas velocidade de transferência e baixa perda de dados quando usados em fibras ópticas
- Dois tipos de conexão:
  - Virtual Path Connection, identificado pelo Virtual Path Identifier (VPI) no pacote
  - Virtual Channel Connection, identificado pelo Virtual Channel Identifier (VCI) no pacote.
  - Um determinado Channel corresponde a um determinado Path



- A inserção de dados nas células é feita pelo protocolo AAL (ATM Adaptation Layer). Está dividido em:
  - Convergence Sublayer (SA) - Controla o fluxo de dados para e desde o SAR sublayer;
  - Segmentation and Reassembly Sublayer (SAR) - Converte dados para células no remetente, e converte células para dados no receptor;
- Fornece dois tipos de conexões:
  - Permanent Virtual Connections (PVC) - Conexões configuradas automáticamente pelo administrador da rede;
  - Switched Virtual Connections (SVC) - Configuradas pelo utilizador receptor através de sinais.

➔ **Ethernet**

- Redes baseadas em ligações P2P (Ponto a Ponto), que usam comutadores de nivel 2;
- Fornece alguns novos protocolos
  - IEEE 802.1s (MTP – Multiple Spanning Trees)
  - IEEE 802.1w (RRSP – Rapid Reconfiguration of Spanning Tree)
  - IEEE 802.17 (RPR – Resilient Packet Ring working group)
  - IEEE 802.3ad (Link Aggregation)
- Apresenta algumas limitações:
  - Suportar um número elevado de clientes
  - Fiabilidade e recuperação de falhas
  - Mecanismos de QoS poderosos
  - Separação do tráfego de clientes

BGP (Border Gateway Protocol)

➔ **Encaminhamento entre sistemas autónomos que usa o protocolo de transporte TCP**

- Todos os pares trocam as suas rotas na primeira sessão estabelecida. Sempre que houver alterações na rede, as rotas têm de ser atualizadas;
- Mesmo AS – IBGP (Internal)
  - Um router nunca encaminha um pacote aprendido por um peer IBGP para outro peer IBGP mesmo que esse caminho seja o melhor (excepto se o router for refletor);
  - Routers IBGP num mesmo AS têm de manter uma sessão IBGP com todos os outros routers IBGP do mesmo AS (mesh - malha) para obter informação de routing sobre redes externas;
  - Algumas redes usam também um IGP como o OSFP;
- Diferentes AS – EBGP (External)
  - Um router reencaminha um pacote aprendido por um peer EBGP para outro peer EBGP ou IBGP
- Faz uso de Path-Vector:
  - O vector transporta a lista dos AS percorridos pelo pacote;
  - Um EBGP peer junta o seu AS ao vector antes de reencaminhar para outro EBGP peer;
  - Um IBGP peer não junta o seu AS ao vector porque vai reencaminhar dentro do seu AS;
- Pode fazer uso de routers Reflector

- Fazem o mesmo que o IBGP faria dentro de um AS

➔ **Tipos de AS:**
- Single-Homed, apenas tem um router fronteira para chegar a redes fora do AS;
- Multi-Homed Non Transit, possui mais de um router fronteira, mas não transporta tráfego de outro AS;
- Multi-Homed Transit, possui mais de um router fronteira e transporta tráfego de outro AS;

➔ **Pacotes BGP:**
- OPEN – Os routers usam mensagens OPEN para estabelecer relações de vizinhança (declaram o nº do AS);
- UPDATE – Mensagem que transporta informação sobre atualizações de encaminhamento entre os routers.
  - Routers Withdrawn – redes IP que não podem ser atingidas;
  - Path Attributes – Definem a rota e politicas de encaminhamento;
  - NLRI (Network Layer Reachability Information) – lista com redes destino anunciadas;
- KEEPALIVE – Se não houver atualização de rotas, os routers trocam mensagens destas para manter a relação de vizinhança;
- NOTIFICATION – Transmitidas em situações de erro ou para terminar ligação;

➔ **Atributos BGP**
- Well-Known Mandatory
  - AS_PATH – quando uma rota passa num AS, o número dele é adicionado a uma lista de AS;
  - Next_hop – endereço IP usado para alcançar router anunciante. Para o EBGP é o endereço IP da ligação entre peers, para IBGP o next-hop EBGP é transportado dentro do AS local;
  - Origin – indica como o BGP aprendeu determinada rota (IGP, EGP, Incomplete);
- Well-Known Discretionary
  - Local Preference – Usado para escolher um ponto de saída do AS local (propagado ao longo do AS);
  - Atomic Aggregate – Alertar routers que algumas rotas específicas foram agregadas noutras menos especificas, sendo as mais especificas perdidas;
- Optional Transitive
  - Aggregator – Informa sobre o AS que fez a agregação, fornecendo o IP do router que originou a agregação;
  - Community – Agregar rotas com propriedades comuns. Podem ser *No-export* (não anunciam a rota aos peers EBGP), *No-advertise* (não anunciam rota a nenhum peer), *Internet* (anunciam rota a todos os routers da Internet);
- Optional Non-Transitive
  - Multi-exit-discriminator – Usado para sugerir um AS a outro AS externo, sendo usado o valor mais baixo de métrica;
- Cisco-Defined
  - Weight – Atributo que determina rota a usar quando existem mais de uma rota para mesmo destino;

➔ **Filtragem BGP**
- Route Filtering – define-se uma access list aplicada aos updates de e para um vizinho;
- Path Filtering – define-se uma acess-list com determinadas condições de entrada e saída;
- Communities – define-se um atributo do Community a aplicar ao update de um router;

➔ **Route Maps**
- Usadas para controlar e modificar informações de encaminhamento (definindo as condições que levam a isso);

➔ **Sincronização**
- Se um SA encaminha tráfego de um SA para outro SA, o BGP não deve anunciar a rota antes que todos os routers desse SA aprendam essa rota por IGP;

➔ **Route Reflector**
- Sem um route reflector, a rede tem de aprender todas as rotas por IBGP mesh;

➔ **Redistribuição de rotas**
- **IGP por BGP –** Simplifica a configuração do BGP, e este vai anunciar apenas rotas internas que possuam conetividade;

- **BGP por IGP –** Todas as rotas internas conhecem as externas, o que vai aumentar o tamanho das routing tables, e evita o uso de rotas internas por omissão;

➔ **Conflitos BGP E IGP –** Podem ser causados por routers internos sem BGP, não redistribuição de rotas BGP por IGP ou rotas IGP por omissão. As soluções são ajustar as rotas IGP, e estabelecer as vizinhanças BGP e routing interno por tuneis IP-IP (manualmente configurados);

Roteamento baseado na fonte – Os pacotes transportam, desde a fonte, uma lista de endereços de routers pela qual eles têm de ir até chegar ao seu destino (usa-se o campo *Options* do datagrama IP).

Rede MPLS – Rede onde os pacotes estão identificados com um label (valores pequenos) do primeiro hop. Os routes encaminham os pacotes conforme o label deles. Isto vai simplificar todo o processo de encaminhamento, simplificando a gestão de rede. Apresenta os seguintes elementos:

- FEC (Forwarding Equivalence Class) – Identificam grupos de pacotes MPLS tratados da mesma forma;
- LSR (Label Switching Router) – Routers do mesmo dominio que formam um dominio MPLS;
- LER (Label Edge Router) – Interagem com o exterior do dominio;
- LSP (Label Switched Path) – Caminho por onde circulam os pacotes numa rede MPLS;
- LDP (Label Distribution Protocol) – Protocolo usado para controlar o FEC, a distribuição de labels e estabelecer e manter LSP's;
- LFIB (Label Forwading Information Base) – Tabela de encaminhamento criada por protocolos de encaminhamento e labels:
- LSP Tunneling – Explicia LSP entre dois LSR que não estão diretamente conectados:
- Multi-Level Label Stack – Pilha FIFO que contém os labels dos pacotes MPLS;

Para descoberta da rede MPLS, os routers mandam pacotes "Hello" entre si para se conhecerem. Mais tarde vão enviando mensagens KEEPALIVE para manterem a conexão. Para estabelecerem um LSP, um LSR upstream manda uma mensagem de label request com FEC para um LSR downstream. Este ao receber o request pode responder de dois modos: ordenado, apenas respondendo com o seu label quando obtiver o label do downstream, ou independente, respondendo mal receba o request. Um LSR pode manter guardados os labels de dois modos: conservativo, onde apenas guarda os labels dos seus next-hops (quando há espaço limitado para labels) ou de modo liberal, guardando quaisquer labels (para adaptações rápidas a mudanças de rotas).

Encaminhamento básico restringido – O objetivo do encaminhamento é determinar o caminho de menor custo (cada link tem um custo) por forma a não violar algumas restrições estabelecidas (largura de banda, atraso, prioridade, etc). Esses caminhos vão ser descobertos, procedendo-de à reserva de recursos ao longo desses caminhos, especificação do LSP e encaminhamento do tráfego.

RSVP (Resource Reservation Protocol) vs LDP - Protocolos com aproximações emergentes/competidoras/duelistas. Normalmente diriamos "Usa LDP para simplicidade, usa RSVP se queres garantir largura de banda".

➔ **LDP -** Ao ligarmos o LDP, as labels são automaticamente anunciadas para cada rota. Temos LSP's instantâneas, labels atribuidas a todas as interfaces, mesmo aquelas que não precisamos. Podemos também incorporar politicas de QoS mas estamos limitados aos bits EXP. As mensagens LDP dividem-se em quatro categorias:
  - Discovery Mesages – anunciar e manter rotas LSP na rede;
  - Session Messages – estabelecer, manter e terminar sessões LDP entre pares;
  - Advertisement Messages – criar, alterar e apagar labels para FEC's;
  - Notification Messages – fornecer informação importante ou sinalizar erros;

➔ **RSVP-TE (Traffic Engineering)** - cria uma LSP cujos parâmetros podem ser configurados manualmente. Caso os parâmetros estejam de acordo com as bases de dados de TE, então a conexão é estabelecida. Pode incorporar também politicas de QoS.

Prioridade LSP – As prioridades do LSP dividem-se em "Setup Priority" e "Holding Priority", ambos com 8 niveis de prioridade. A prioridade é fulcral sempre que na rede um LSP requer requisitos não disponiveis, ou então em casa de falha na rede. Uma LSP pode "roubar" recursos de LSP existentes cuja "Holding Priority" < "Setup Priority"

MPLS-VPN (Virtual Private Network) – Uma VPN é uma rede segura formada entre nós que podem comunicar de forma segura por canais seguros partilhados.

- ➔ MPLS L3 VPN – Fornece capacidade de desenvolver e administrar serviços de camada 3 a clientes de négocio;
- ➔ MPLS L2 VPN – Conectividade entre clientes ao nivel 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 construida com base numa já existente. Pode consistir em software de encaminhamento instalado em sites desejados, ligados por tuneis 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 conteudo). Os CDN fornecem grande parte do conteúdo online hoje em dia (ficheiros descarregaveis, aplicações, ficheiros web, etc). Um operador CDN é pago pelos servidores originais para fornecerem conteudo, 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;
- **Distribuida/Flooding –** Qualquer nó na rede pode atuar como servidor para upload/download (Gnutella). Tem como grandes vantagens o bom tempo de resposta e escabalibilidade, 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;
- **Hibrida –** Misto de centralizada e distribuida, 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 construidas de duas formas:

- **Destruturadas** – Construidas quando a rede overlay é estabelecida arbitrariamente. Quando um par quer encontrar um pedaço especifico 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 unica saída com base em várias entradas CSRC. O SSRC da saída vai ser o do mixer.

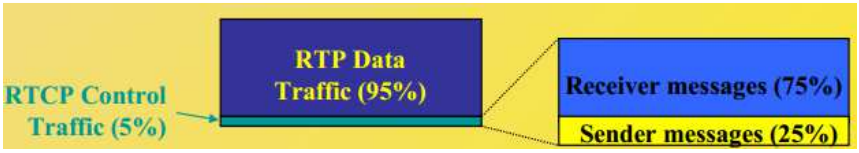
Um cabeçalho RTP contempla alguns atributos importantes:

- **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 contribuiram 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 monotorização 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 caracteristica 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 estatisticas para o emissor;
  - **RR (Receiver Report) –** Envio de estatisticas 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 enfiar a informação, porque a codificação é sempre sensivel 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 encapsultado 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 Protocolo) – 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, obtem 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 Resourse Identifier) –** Traduzido pelo servidor proxy, para o endereço do UA do utilizador. Um mesmo utitilizador pode ter vários endereços UA

As mensagens SIP dvidem-se nos seguintes métodos:

- **REGISTER –** Registar um UA no serviço de localização;
- **INVITE –** Estabelecer ou alterar os parametros de uma sessão;
- **200 OK –** Sinalizações de confirmação por parte do emissor;
- **ACK –** Confirmar a recepção 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 parametros para se iniciar uma sessão multimedia (SIP), como o anuncio 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 disponiveis, 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 exister, 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 inicio 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 atribuido 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 numero 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;
- **Worldwilde (Sattelite) –** 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 TDAM/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 caractéres 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 especificos 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 distribuidos por canais fisicos. Um canal fisico consiste num espaço de tempo definido, num canal especifico. Assim o canal fisico trata do espaço de tempo, e o canal lógico trata da informação transportada pelo canal fisico. 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 43.2kpbs). 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 publica, 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 Telecomunication 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 extensivel. No entanto é muito simples, não é escalável, o uso de polling cria muito overhead, tem muitas especificações.

Sistema Baseado em Politicas – Dividido em:

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

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 politicas 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 especifica, 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 procolos 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 (Telecomunications 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 disponiveis 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 criticos de controlo da rede. Pode identificar, agir, juntar informação, fornecer comandos aos sistemas para iniciarem, manter ou terminar conxeões;
- **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).