
COMPUTADORES 1

Técnico de Eletrónica Automação e Computadores

ENSINO PROFISSIONAL

UFCD - 6127

INTRODUÇÃO ÀS REDES E TRANSMISSÃO DE DADOS



Conteúdo

| | |
|---|----|
| Conceitos básicos | 5 |
| Redes de dados e comunicações..... | 5 |
| Importância das redes de dados | 6 |
| Áreas de aplicação e perspectivas de evolução | 8 |
| Modos de comunicação | 8 |
| Componentes de um sistema de comunicação..... | 10 |
| Hardware e software de rede | 10 |
| Transmissão de dados | 11 |
| Transmissão em paralelo e em série | 11 |
| Transmissão simplex, half-duplex e full-duplex..... | 13 |
| Transmissão por difusão e ponto a ponto | 13 |
| Transmissão em baseband e em broadband | 14 |
| Ligações síncronas e ligações assíncronas | 14 |
| Transmissão síncrona..... | 14 |
| Transmissão assíncrona | 15 |
| Transmissão sem fios <i>ou wireless</i> | 16 |
| Infravermelhos | 16 |
| Ondas de rádio..... | 16 |
| Micro-ondas..... | 16 |
| Modulação em amplitude, frequência e fase | 16 |
| Grandezas e medidas | 18 |
| Decibel (DB) | 18 |
| Largura de banda | 19 |
| Throughput | 21 |
| Bit Rate | 21 |
| Técnicas de codificação | 22 |
| NRZ..... | 22 |
| NRZ Unipolar..... | 22 |

| | |
|--|----|
| NRZ Polar | 22 |
| NRZ Bipolar (AMI) | 22 |
| RZ | 23 |
| RZ Unipolar | 23 |
| RZ Polar | 23 |
| RZ Bipolar (AMI) | 24 |
| Técnicas de deteção e correção de erros em transmissões digitais | 24 |
| Deteção de erros | 24 |
| Verificação de paridade | 25 |
| Checksums | 25 |
| Correção de erros | 26 |
| Técnicas de compressão de dados | 27 |
| Compressão com perdas | 27 |
| Compressão sem perdas | 28 |
| Natureza dos dados | 28 |
| A informação | 30 |
| O que é a informação | 30 |
| Qualidade da informação | 30 |
| Tipos de informação | 32 |
| Estádios de informação | 32 |
| Informação digital | 33 |
| Classificação das redes de computadores | 34 |
| Classificação das redes quanto à extensão geográfica | 34 |
| LAN | 34 |
| MAN | 35 |
| WAN | 35 |
| Outras classificações quanto a extensão geográfica | 36 |
| Classificação de redes quanto à hierarquia | 36 |
| Redes ponto-a-ponto | 36 |

| | |
|---|----|
| Redes cliente-servidor | 37 |
| Meios físicos de transmissão | 37 |
| Cabos elétricos..... | 38 |
| A importância das atividades de normalização | 45 |
| Noção de norma e de normalização | 45 |
| Organizações de normalização: ISO, ISOC, IEC, IEEE..... | 46 |
| Padrões e arquiteturas de redes..... | 47 |
| As tarefas dos computadores na rede | 50 |
| Servidores de ficheiros e impressoras | 50 |
| Servidores de DHCP | 51 |
| Servidores de DNS | 51 |
| Servidores de email | 51 |
| Servidores de base de dados | 51 |
| Servidores de fax | 51 |
| Principais dispositivos de uma rede | 52 |
| Intranet e Extranet | 53 |
| Topologias | 54 |
| Anel (<i>ring</i>) | 54 |
| Barramento (<i>bus</i>) | 54 |
| Estrela (<i>star</i>)..... | 55 |
| Malha (<i>mesh</i>) | 55 |
| Ponto-a-ponto (<i>point-to-point</i>) | 56 |
| Árvore (<i>tree</i>)..... | 56 |
| Modelos de Referência OSI | 56 |
| Descrição funcional das camadas..... | 57 |
| Camada 1 – Física..... | 57 |
| Camada 2 – Enlace | 57 |
| Camada 3 – Rede | 57 |
| Camada 4 – Transporte..... | 58 |

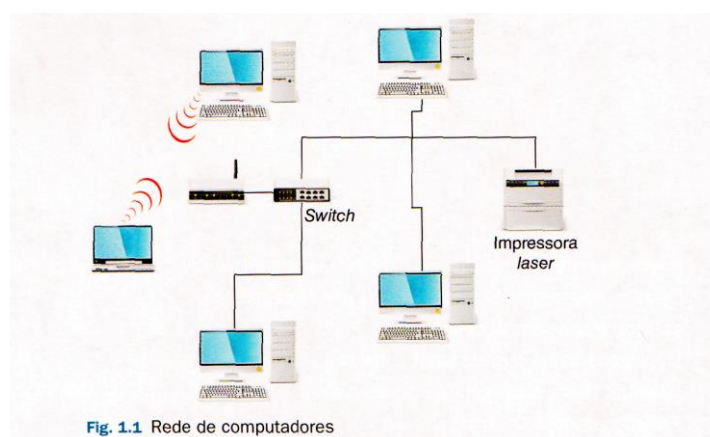
| | |
|-------------------------------|----|
| Camada 5 – Sessão | 58 |
| Camada 6 – Apresentação | 58 |
| Camada 7 - Aplicação..... | 58 |
| Arquitetura TCP/IP | 59 |
| Camada de Acesso à Rede | 59 |
| Camada Internet | 59 |
| Camada de Transporte..... | 59 |
| Camada de Aplicação | 59 |
| EXERCÍCIOS PROPOSTOS | 60 |
| Referências..... | 67 |

CONCEITOS BÁSICOS

REDES DE DADOS E COMUNICAÇÕES

Uma rede de computadores é constituída por dois ou mais computadores interligados por cabo, por linhas telefónicas ou por comunicações sem fios. Na rede podem ser adicionados outros tipos de equipamento, como, por exemplo, periféricos (impressoras, modems, fax, etc.), que depois de partilhados podem ser acedidos pelos utilizadores a partir dos diferentes postos de trabalho.

Tanto em grandes como em pequenas empresas ou organizações, as vantagens da interligação em rede de equipamento informático são tão evidentes que o uso isolado de um computador quase não se verifica. Mesmo em habitações, este tipo de tecnologia em rede começa a ser cada vez mais visível através da rede sem fio.



Podemos definir uma **rede** da seguinte forma:

Dois ou mais computadores ligados entre si, por meios eletrónicos, com o objetivo de trocarem informação de forma rápida e fácil, permitindo aos utilizadores a partilha de equipamentos e recursos (aplicações, ferramentas de comunicação, bases de dados...).

ou **conforme a Norma NP3003-1:**

Rede constituída por nós de processamento de dados interligados com o fim de permitirem a comunicação de dados.

ou ainda:

Conjunto de dispositivos conectados entre si com a finalidade de partilharem recursos.

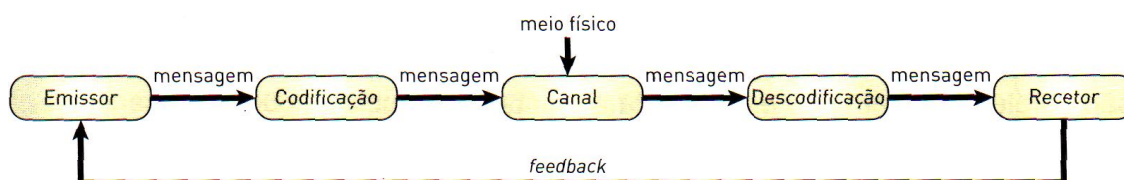


Fig. 1.2 Processo de comunicação por rede

Resumindo, podemos afirmar que uma rede é um processo de comunicação eletrónico que permite transmissão e receção de dados, tais como caracteres, ficheiros, voz, vídeo, entre um equipamento emissor e outro recetor.

IMPORTÂNCIA DAS REDES DE DADOS

Nesta nova era, a da informação, as redes informáticas têm uma importância fundamental dado que permitem uma série de vantagens, que passamos a descrever:

- Imagina que tens em casa, ou num escritório, dois ou mais computadores e que para imprimir os trabalhos necessitas de uma impressora para cada um dos computadores. Esta opção, para além de dispendiosa, torna o sistema suscetível a avarias, devido ao maior número de equipamentos. No caso de as impressoras serem diferentes a situação piora, pois teríamos de ter os consumíveis para cada um dos modelos de impressora. Outra opção seria ter uma só impressora e mudá-la para o computador em que se pretende imprimir cada vez que necessitasse de o fazer. Esta solução, além de pouco prática, provocaria um desgaste maior do material, devido às constantes mudanças do equipamento. Para além disto, em situações de impressão em simultâneo em computadores diferentes, teríamos de aguardar que fosse impresso um trabalho e de seguida mudar a impressora para o outro computador.
- A opção ideal seria termos uma impressora de melhor qualidade e partilhá-la em rede com todos os computadores desse segmento da rede. Uma impressora só imprime um documento de cada vez, mas o sistema operativo de rede gere os pedidos de impressão, colocando-os em fila de espera do tipo FIFO (*First In First Out*).
- Em situações onde se verifique a necessidade de ter dois ou mais computadores com acesso à Internet, podemos ter apenas um *modem* e um acesso, que será partilhado por todos os computadores da rede.
- É possível partilhar dados num disco rígido de um computador disponibilizando um determinado documento para este poder ser utilizado por um conjunto de utilizadores. Assim, evita-se a repetição de tarefas e de informação.
- Os utilizadores podem aceder remotamente a programas e a bases de dados sem que seja necessário instalá-los localmente.
- As bases de dados podem ser partilhadas. Podemos armazenar todo um conjunto de dados e mais tarde efetuar uma pesquisa para obtermos os elementos necessários; por exemplo, os dados de um cliente.
- Estando as pessoas interligadas em rede com computadores, podem ser criados trabalhos em equipa utilizando as redes locais, ou a Internet, onde existem atualmente diversas redes sociais.
- Tornou-se possível a troca de informação entre os utilizadores sem a necessidade de utilizar os meios

tradicionais de telecomunicações. Assistimos atualmente à massificação do correio eletrónico e dos *chats* de voz e vídeo.

- É possível efetuarem-se algumas tarefas de manutenção do parque informático remotamente, evitando-se a deslocação de pessoas.
- As cópias de segurança tornam-se mais eficazes. Se todas as pessoas guardarem os trabalhos num determinado disco que é partilhado, e não individualmente, em cada um dos computadores, é mais fácil criar as cópias de segurança, pois apenas se tem de ir buscar a informação a um local. No entanto,
- para que isto seja possível e resulte, é necessário criarem-se políticas de segurança que impeçam que um dado utilizador apague os dados de outro.
- Diminuição de custos: do que foi referido anteriormente irá verificar-se uma grande diminuição de custos relativamente à situação de não existência de rede.

Atualmente, existem dois tipos de rede de dados: a **rede privada** e a **rede pública**. As redes privadas são redes, configuradas para permitir a transmissão de dados dentro de uma organização.

Ao contrário da rede de dados privada, a rede pública de dados é acessível tanto a clientes residenciais como a organizacionais. A configuração de uma rede pública implica a utilização de múltiplos servidores e a sua ligação à rede através de diferentes processos. O acesso à rede de dados pública requer algum tipo de subscrição, através da qual o ISP (*Internet Service Provider*) fornece ao cliente os equipamentos e as credenciais (nome de utilizador e palavra-passe) de acesso. Esta ligação permite o acesso a uma infinidade de serviços "residentes" na Internet, bem como o *download* e o *upload* de dados, a criação e a recuperação de cópias de segurança (*backups*), entre outros.

Apesar de todas estas vantagens, há problemas que surgem com a ligação de computadores em rede:

- Com a interligação dos computadores, a velocidade de propagação de vírus informáticos é enorme. É muito fácil receber-se uma mensagem vinda por correio eletrónico contendo um vírus, que, automaticamente, envia novas mensagens com o referido vírus para todas as pessoas que se encontram na nossa lista de endereços. Com este modo de propagação rápida, o controlo de vírus torna-se mais difícil.
- Há a possibilidade de intrusão não autorizada. Apesar dos sistemas de segurança, há sempre um *hacker* que consegue romper estas seguranças e entrar no sistema. Está mais que provado que muitos sistemas considerados invioláveis já foram alvo de intrusões.
- O sistema torna-se mais complexo, exigindo pessoal mais especializado para a manutenção do mesmo. O grau de dificuldade em gerir um computador isolado é muito inferior à manutenção de uma rede informática, com diversos computadores.

O desenvolvimento das tecnologias de comunicação avança a uma velocidade estonteante e, hoje em dia, apesar das desvantagens apresentadas, o futuro de uma organização, e mesmo de habitações pessoais, passa

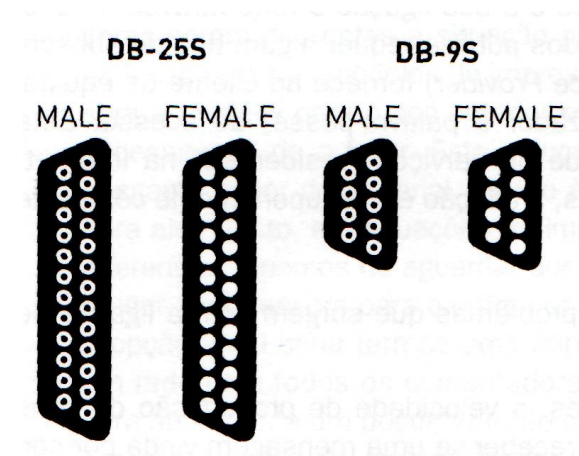
pela interligação dos sistemas em rede. No caso particular de uma habitação, os sistemas de iluminação, televisão, telefone e mesmo dos eletrodomésticos podem estar interligados à rede informática, tornando possível gerir esses equipamentos a partir de um computador remoto.

ÁREAS DE APLICAÇÃO E PERSPETIVAS DE EVOLUÇÃO

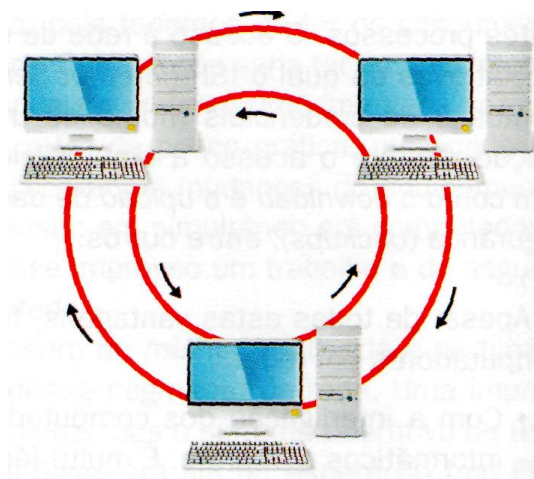
Os sistemas informáticos evoluíram muito nos últimos 50 anos e originaram uma evolução tecnológica sem precedentes. O fabrico de computadores com grande capacidade de processamento e o acesso facilitado à informação através da Internet são sinais de que este processo não irá ficar por aqui...

Verificámos, na década de 60 do século XX, o aparecimento da comunicação série RS232 a velocidades que variavam entre 1 kbps e 10 kbps; em meados da década de 70, surge a comunicação série *full-duplex* com velocidades de 100 kbps a 1 Mbps; nos anos 80, desenvolveram-se os padrões Ethernet a 10 Mbps, o *token ring* com velocidades entre os 4 Mbps e 16 Mbps e o FDDI (*Fibre Distributed Data Interface*) a 100 Mbps; na década de 90, o *fast ethernet* a 100 Mbps, o ATM (*Asynchronous Transfer Mode*) com velocidades de 155 Mbps a 622 Mbps e ainda o gigabit Ethernet a 1 Gbps.

*bps - bit por segundo



Portas RS232

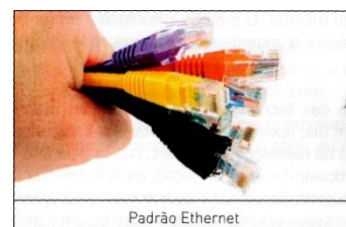


FDDI

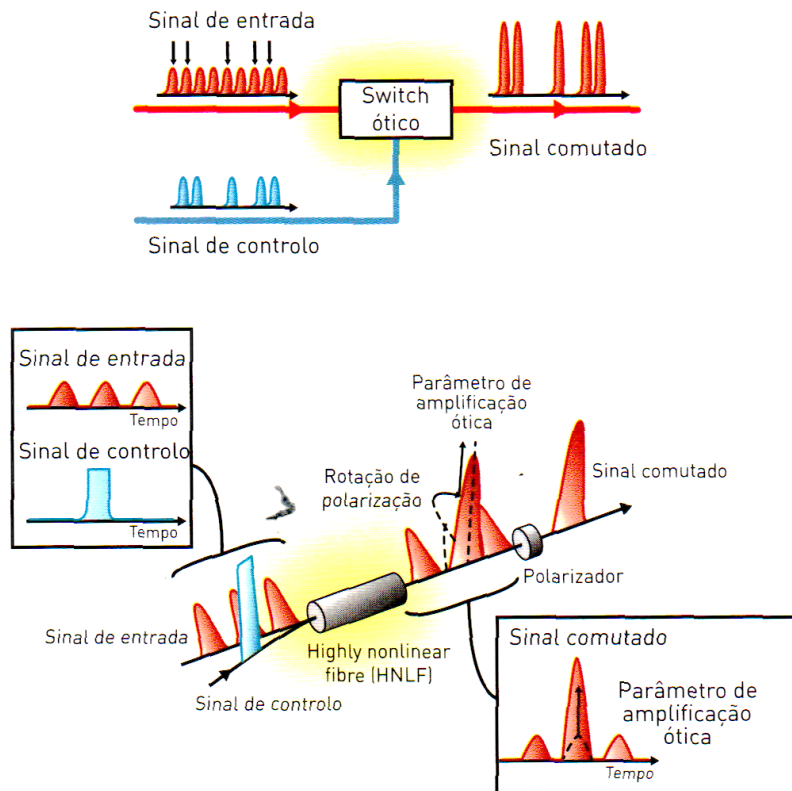
MODOS DE COMUNICAÇÃO

Assistimos hoje, graças à utilização em grande escala da fibra ótica, a novos desenvolvimentos, nomeadamente a Ethernet a 10 Gbps e o ATM a 2,4 Gbps. Prevê-se ainda, nos próximos anos, o aparecimento da rede a velocidades que podem chegar aos 1000 Gbps, isto é, 1Tbps.

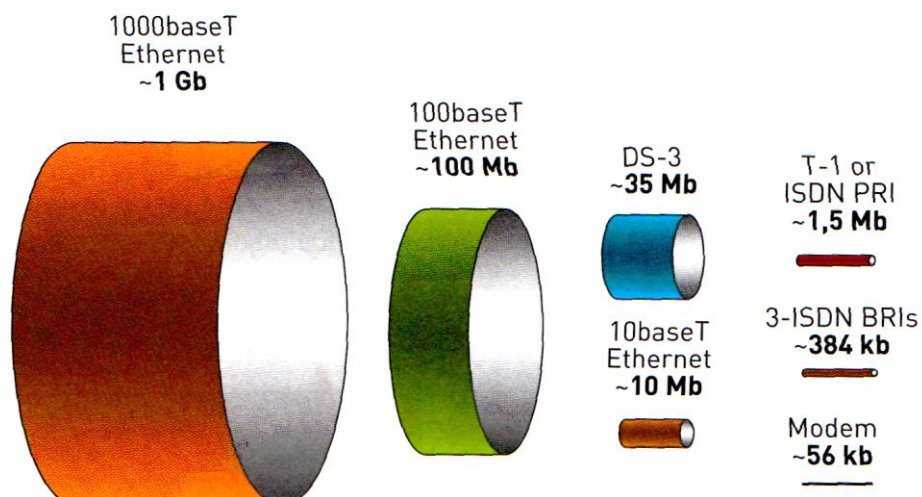
Os desenvolvimentos verificados nas redes deveram-se em *grande medida* à utilização de protocolos de comunicação mais leves, mais robustos e ainda mais adaptativos, o que implicou uma melhoria substancial da qualidade de serviço.



Verificaremos dentro de alguns anos as redes **ubíquas** com infraestruturas de comunicação inteiramente éticas.



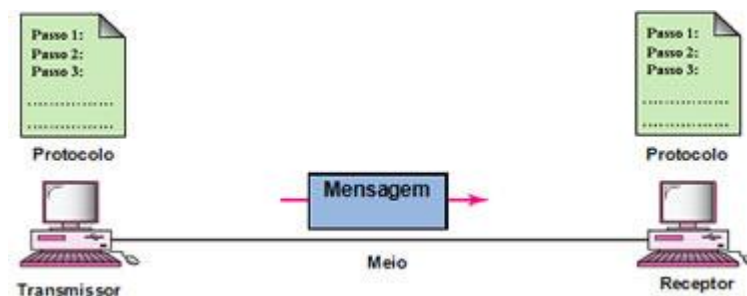
Nas redes informáticas, existem diversos meios de transmissão: linha telefónica, cabo coaxial fino, cabo coaxial grosso, cabo UTP/STP e fibra ótica. Atualmente, é muito utilizados o cabo UTP cat 6 que pode atingir 1 Gbps, enquanto a fibra, o melhor meio de transmissão para as redes informáticas, tem uma largura de banda que pode variar entre os 200 Mbits e os 10 Gbits.



COMPONENTES DE UM SISTEMA DE COMUNICAÇÃO

Comunicar sempre foi uma necessidade humana. Desde sempre o ser humano desenvolveu formas de comunicar entre si. Um sistema básico de comunicação de dados é constituído essencialmente por: mensagem, emissor, recetor, meio ou canal e protocolo.

- **Mensagem:** é a informação a ser transmitida. Pode ser constituída de texto, números, figuras, áudio e vídeo – ou qualquer combinação desses.
- **Emissor:** é o dispositivo que envia a mensagem de dados. Pode ser um computador, uma estação de trabalho, um telefone, uma câmara de vídeo e assim por diante.
- **Recetor:** é o dispositivo que recebe a mensagem. Pode ser um computador, uma estação de trabalho, um telefone, uma câmara de vídeo e assim por diante.
- **Meio:** é o caminho físico por onde viaja uma mensagem originada e dirigida ao recetor.
- **Protocolo:** é um conjunto de regras que governa a comunicação de dados. Ele representa um acordo entre os dispositivos que se comunicam.



A eficiência de um sistema de comunicação de dados depende fundamentalmente de três características:

- **Entrega (delivery):** o sistema deve entregar os dados ao destino correto. Os dados devem ser recebidos somente pelo dispositivo ou usuário de destino.
- **Confiabilidade:** o sistema deve garantir a entrega dos dados. Dados modificados ou corrompidos na transmissão são pouco úteis.
- **Tempo de atraso:** o sistema deve entregar os dados num tempo finito e predeterminado. Por exemplo, no caso de transmissões multimídia, como vídeo, os atrasos podem criar entraves na comunicação, assim, os dados que eles devem ser entregues imediatamente ao momento em que foram produzidos, isto é, sem atrasos significativos.

HARDWARE E SOFTWARE DE REDE

A interligação dos computadores em rede apenas é possível utilizando hardware e software adequados.

O hardware utilizado para ligar um computador em rede é o seguinte:

- computadores;

- placas de rede;
- cabos de rede com fichas RJ45;
- dispositivos de interligação (switch, access point, router);
- periféricos que vão ser partilhados (modems, routers, impressoras, scanners, entre outros).

O software necessário à interligação dos computadores é o seguinte:

- sistema operativo;
- programas de rede - alguns só já incluem software de rede;
- drivers ou controladoras das placas de rede;
- protocolos de comunicação.

TRANSMISSÃO DE DADOS

Chegou a altura de nos debruçarmos sobre o modo como os dados são transmitidos ao longo dos canais de transmissão. Estudaremos, ainda, alguns conceitos associados à transmissão.

TRANSMISSÃO EM PARALELO E EM SÉRIE

As transmissões de dados de um computador para outro computador ou para outro dispositivo podem ser efetuadas de dois modos distintos:

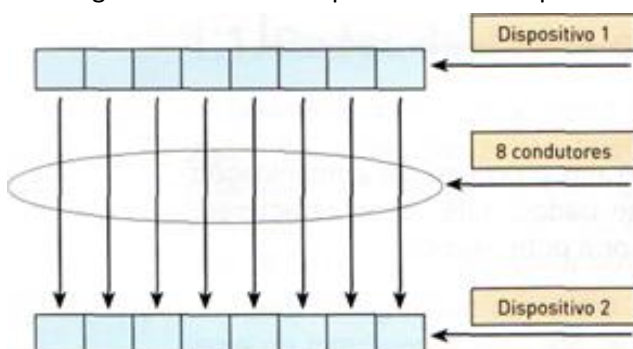
Modo paralelo - neste caso são enviados vários bits ao mesmo tempo;

Modo série - os bits necessários para a transmissão de uma mensagem são enviados um a um.

Se bem que uma transmissão em paralelo consiga transmitir mais informação no mesmo período de tempo, em redes de computadores as transmissões são sempre feitas em série. A razão principal deve-se a que as transmissões em paralelo exigem cabos com maior número de fios condutores e, por isso, mais caros.

Além disso, essas transmissões colocam problemas de sincronização na receção dos dados e estão mais sujeitas a interferências causadoras de erros. A transmissão paralela também não é adequada a grandes distâncias.

A figura 1.3 ilustra de que modo um dispositivo transmite os *bits* em paralelo para outro dispositivo; por



exemplo, da porta paralela de um computador para uma impressora. Os 8 *bits* de cada bit são transmitidos em simultâneo por oito condutores.

Como nas redes de computadores a transmissão é em série, vamos aprofundar um pouco os conceitos sobre este método de envio de dados.

Figura 1.3 - transmissão de dados

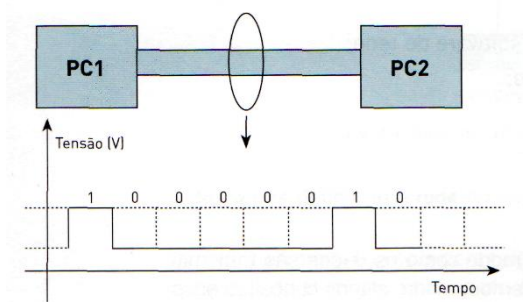


Fig. 1.4 Transmissão em série

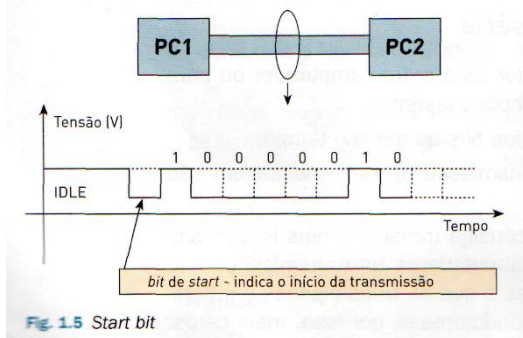


Fig. 1.5 Start bit

A transmissão em série permite que dois dispositivos comuniquem entre si, desde que obedeçam a protocolos bem definidos, isto é, a leis que regem as comunicações entre os dispositivos. Duas pessoas, quando falam, só se entendem se utilizarem a mesma linguagem.

Os dados a transmitir ao longo de uma rede são emitidos sob a forma de sinais elétricos. Esses sinais apresentam uma propriedade inerente, que é a tensão elétrica. Como os sistemas informáticos só entendem a linguagem binária, O ou I, tem de ser feita uma associação, uma correspondência entre as tensões e os códigos binários.

Os protocolos estão, em geral, definidos por normas internacionais (por exemplo, a norma RS 232), que estabelecem as relações entre os *bits* e os níveis de

tensão elétrica (por exemplo, 2,4 V ou 0,4 V - 3 V ou + 3 V), para

o formato dos dados a transmitir e para o débito de transmissão de *bits* por unidade de tempo.

A figura 1.4 ilustra de que modo se transmite uma sequência de *bits* entre dois dispositivos PC1 e PC2 pelo modo série.

Assim, os *bits* são representados por impulsos retangulares, como mostra a figura 1.5, em que o valor '1' corresponde a um certo nível de tensão elétrica e o valor '0' a outro nível, sendo estes definidos pela norma utilizada.

Quando a transmissão está em repouso, o impulso está no nível correspondente ao valor 1.

Quando um dispositivo começa a transmissão é enviado um primeiro *bit* de controlo, a que se dá o nome de **start bit**, que indica o início de uma transmissão (figura 1.5).

Depois do *start bit* são transmitidos os *bits* do carácter a enviar, seguidos de um **bit de paridade** e de 1 a 2 *bits de stop*, que indicam o fim da transmissão.

O bit de paridade, que surge na figura 1.6, permite uma deteção elementar de erros na transmissão que ocorram num dos bits do byte enviado.

Por exemplo, se enviarmos o código correspondente ao carácter 'B' e ocorrer um erro no último bit, o recetor recebe o código correspondente ao carácter 'C'. Uma solução é acrescentar-se informação que permita ao recetor detetar se houve erro num b/t.

Esta consiste num bit extra, o **bit de paridade**.

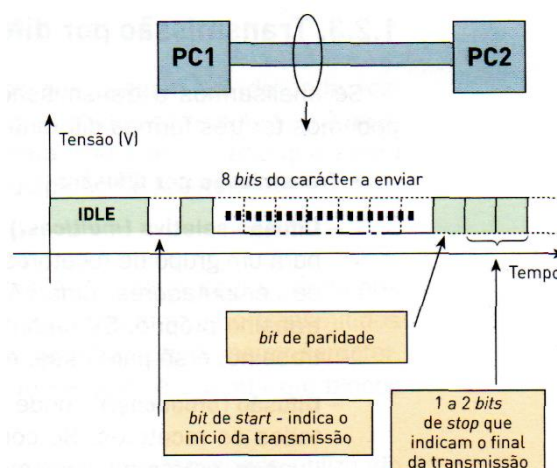


Fig. 1.6 Grupo de bits a transmitir

Há dois modos possíveis, definidos no início da transmissão: a paridade **par** ou **ímpar**. No caso da paridade ímpar, envia-se, em vez do código de 'B', o código que se vê na figura 1.8.

Se o recetor receber **101000011**, deteta um número par de bits ale verifica ter havido um erro. Será, então, pedido ao emissor que volte a transmitir o carácter. Este método não deteta erros se houver múltiplas trocas de bits que deixem o total a ímpar.

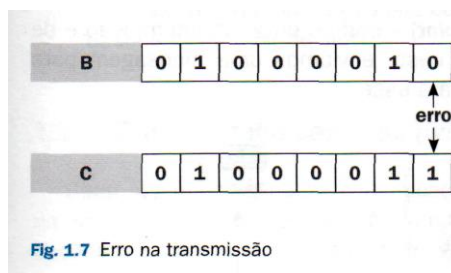


Fig. 1.7 Erro na transmissão

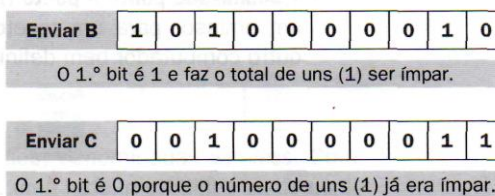


Fig. 1.8 Bit de paridade ímpar

TRANSMISSÃO SIMPLEX, HALF-DUPLEX E FULL-DUPLEX

O transporte de informação e de dados ao longo de canais de comunicação pressupõe a existência de, pelo menos, um emissor e um recetor. A comunicação entre emissores e recetores pode ocorrer de três formas, tendo em conta a direcionalidade e a simultaneidade:

Simplex – quando a comunicação ocorre apenas num sentido. Exemplo deste tipo de transmissão é o da transmissão de sinais televisivos, onde um emissor só emite e o recetor só recebe.

Half-duplex - quando a comunicação se faz nos dois sentidos, mas não simultaneamente. É o caso dos *walkie-talkies*. Para que possamos comunicar com estes aparelhos temos de respeitar uma sinalização para libertar o canal.

Full-duplex - quando a comunicação pode ocorrer simultaneamente nos dois sentidos, isto é, podemos enviar e receber mensagens ao mesmo tempo. É o exemplo do telefone, com o qual podemos falar e ouvir simultaneamente.

TRANSMISSÃO POR DIFUSÃO E PONTO A PONTO

Se analisarmos a transmissão de dados quanto ao número de destinatários, podemos ter três formas diferentes de a fazer:

Transmissão por difusão;

- ⇒ **Difusão seletiva (multicast)** - onde a informação é enviada simultaneamente para um grupo de recetores bem definido. Suponhamos que temos uma rede de computadores, uma LAN, com 5 salas de aula, cada uma no grupo de; trabalho próprio. Se pretendemos enviar uma mensagem para um grupo de trabalho, e só para esse, estamos a fazer uma difusão seletiva
- ⇒ **Difusão (broadcast)** - onde a informação é transmitida simultaneamente para todos os recetores. Se considerarmos a mesma rede do exemplo anterior, quando enviamos uma mensagem para todos os computadores da rede estamos a fazer uma difusão generalizada.

Transmissão ponto a ponto (point to point) - onde o envio da informação é de um emissor para um recetor.

Neste caso, enviamos uma mensagem para outro computador bem definido e só para esse.

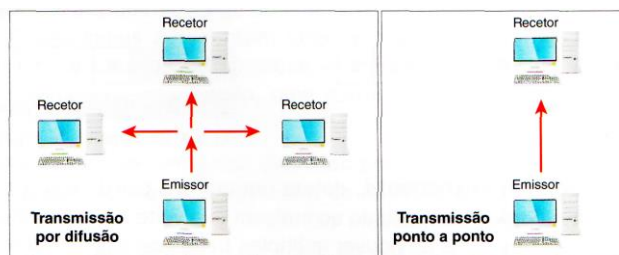


Fig. 1.10 Transmissão por difusão e ponto a ponto

TRANSMISSÃO EM BASEBAND E EM BROADBAND

Para transmitir dados através dos cabos utilizam-se duas técnicas:

Transmissão em banda-base (*baseband*) - esta técnica de transmissão é a mais utilizada nas redes do tipo LAN. Trata-se de uma transmissão em que o sinal faz uso de toda a banda disponível, ou seja, toda a capacidade de comunicação do canal é utilizada para transmitir um único, **sinal digital de dados** (veremos estes sinais mais adiante). Os sinais digitais circulam a uma frequência única pelo cabo. Os sinais fluem sob a forma de impulsos descontínuos de eletricidade ou luz. O fluxo de sinais digitais na *baseband* pode ser bidirecional.

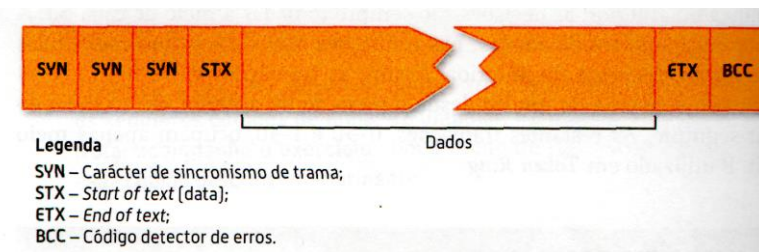
Transmissão em banda larga (*broadband*) - esta técnica de transmissão é mais complexa e mais flexível. Um simples cabo pode transportar múltiplos canais de informação, mas **a informação tem de ser analógica** (veremos os sinais analógicos mais adiante). Essa técnica permite que, ao mesmo tempo, circulem sinais de voz (telefone), vídeo (TV) e dados (computador), ou seja, ela permite a utilização de vários canais ao mesmo tempo (cada um com a sua frequência). Estes sinais fluem na forma de ondas eletromagnéticas nos cabos ou nas fibras óticas. O fluxo de sinais em broadband é unidirecional. Esta técnica é utilizada no acesso à Internet do tipo ADSL e por cabo.

LIGAÇÕES SÍNCRONAS E LIGAÇÕES ASSÍNCRONAS

Um sistema de comunicação interliga um emissor e um recetor através de um canal. Entre eles é estabelecida uma ligação que poderá ser: síncrona ou assíncrona. A forma como o recetor consegue ler os dados transmitidos pelo emissor depende destes tipos de ligações.

TRANSMISSÃO SÍNCRONA

A palavra síncrona indica a presença de um relógio. Este será o responsável por sincronizar emissor e recetor durante a transmissão de informação. O sincronismo permite ao recetor saber quando deve começar a ler os dados e quando deve parar. Conta também com uma verificação de erros do tipo CRC (será explicado no ponto 9.1) que, no caso de erro na transmissão do bloco de dados, garante uma retransmissão da informação. Na figura seguinte é possível observar o formato de uma trama de dados usada numa transmissão síncrona.



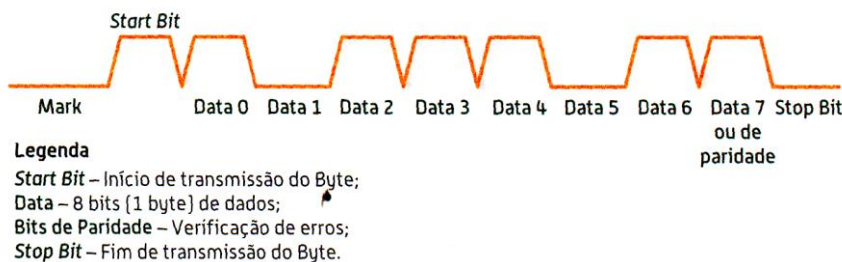
Estrutura de uma trama síncrona

Como é visível, o início de leitura dos dados no recetor ocorre após a leitura do campo STX, que indica o início de transmissão. Neste momento, o recetor sabe que tem de ler os dados enviados pelo emissor até que apareça o campo ETX, que indica o final da transmissão.

Este tipo de transmissão permite que uma grande quantidade de dados (blocos) seja transmitida de uma só vez e ao longo de grandes distâncias, tornando-se **muito eficiente**. Geralmente é usada em *Ethernet*.

TRANSMISSÃO ASSÍNCRONA

Este tipo de transmissão diz-se assíncrona visto não usar um *relógio* de sincronismo para a transmissão dos dados. Sem a presença de um relógio para indicar ao recetor quando deve ler a informação proveniente do emissor é necessário utilizar marcadores (*flags*) que desempenhem essa função. Vejamos uma trama de dados transmitida no modo assíncrono com as *flags* necessárias.



Estrutura de uma trama assíncrona

O recetor ao ler o *Start Bit* (flag inicial) sabe que a partir deste terá um byte (8 bit) de dados para ler. Nesse byte, o último bit poderá contar com um bit de paridade que irá fazer a verificação de erros. O *Stop Bit* (flag final) indica que o byte de dados terminou de ser transmitido. Devido a este cabeçalho adicional, necessário para o controlo, torna a transmissão assíncrona menos eficiente que a transmissão síncrona, não sendo por isso, usado para a transmissão de grandes quantidades de informação e entre grandes distâncias. Possui como principais vantagens apresentar baixo custo e fácil configuração. Este tipo de ligação é muito utilizado quando se pretende configurar equipamentos de rede através de porta série.

No capítulo seguinte, será explicado como funcionam os códigos detetor de erros, inclusive o Bit de Paridade presente na posição Data7.

TRANSMISSÃO SEM FIOS *OU WIRELESS*

Cada vez mais se utiliza comunicações sem fios, denominadas *wireless*. Com um simples comando de televisão, um telemóvel, uma rede informática ou comunicações por satélite, a liberdade de movimentos é incrementada.

No caso particular de redes locais (LAN), estão a surgir novas tecnologias que substituem, em muitos casos, os tradicionais cabos elétricos, tornando mais flexível o posto de trabalho dentro da organização. Ter o computador de secretária "agarrado" ao cabo da rede informática começa a ter os dias contados.

Vamos analisar algumas das tecnologias sem fios existentes nas redes informáticas.

INFRAVERMELHOS

Quando se utiliza um comando de televisão, já se está a utilizar este tipo de transmissão de sinal sem fios. O transmissor e o recetor têm de estar na linha do sinal, caso contrário a comunicação é perdida. Estes sinais trabalham em distâncias curtas, que podem ir até aos 30 m.

ONDAS DE RÁDIO

As ondas de rádio são do mesmo tipo das utilizadas nas transmissões de rádio, onde o emissor espalha o sinal num dado raio de ação e o recetor que detetar e reconhecer esse sinal pode recolher essa informação. Neste caso, podem existir obstáculos entre o emissor e o recetor, tornando ainda mais flexível a comunicação. Podem ter alcances de 70 km.

MICRO-ONDAS

Este tipo de ondas não pode ter obstáculos entre os pontos de comunicação. As micro-ondas são utilizadas em transmissões em redes de área metropolitana (MAN). São também utilizadas em redes do tipo WAN, em satélites de comunicações, que são transmissores de sinais entre bases terrestres. Essas bases têm de ter antenas parabólicas para enviarem e receberem os dados. Os satélites de comunicações estão posicionados em órbitas geostacionárias e rodam a uma velocidade constante relativamente à da Terra. Este tipo de satélites encontra-se entre os 30 e 40 km de altitude em relação à Terra.

MODULAÇÃO EM AMPLITUDE, FREQUÊNCIA E FASE

Um sinal analógico apresenta, caracteristicamente, variações de amplitude, frequência e fase. Estas características são amplamente evidenciadas em sinais rádio e televisivos. Para garantir que a transmissão analógica ocorre de modo mais uniforme utiliza-se a modulação. Por definição, modulação é o processo pelo qual uma onda portadora analógica (sinal elétrico que vai transportar a informação) pode ser alterada, de modo a apresentar um padrão uniforme para a transmissão de dados. O equipamento responsável pela modulação chama-se modem. Este, por definição, é um dispositivo eletrónico que modula um sinal analógico numa determinada faixa de frequência (no emissor), pronta a ser transmitida e que desmodula o sinal analógico para a faixa de frequência original que contém a informação (no recetor).

As modulações analógicas assentam nos três parâmetros que usualmente variam num sinal analógico. Existem três tipos de modulações analógicas:

- Modulação em amplitude (AM - *Amplitude Modulation*);
- Modulação em frequência (FM - *Frequency Modulation*);

- Modulação em fase (PM - *Phase Modulation*).

O que aconteceria se não se usasse a modulação? Quando falamos deste tipo de transmissão falamos de ondas eletromagnéticas irradiadas por antenas. As antenas necessitam de ter um comprimento de pelo menos um décimo do comprimento de onda do sinal, o que significa que por vezes teríamos de contar com antenas de quilómetros para podermos receber um sinal de baixa frequência como, por exemplo, a voz.

Leia com atenção o seguinte exercício:

EXERCÍCIOS RESOLVIDOS

Sabendo que o comprimento de onda $\lambda = VT$ onde v é equivalente à velocidade da luz no vazio $v = 3 \times 10^8 \text{ ms}^{-1}$ e que T é o período da onda a transmitir, verifique qual o tamanho mínimo da sua antena $[L]$ de modo a que consiga receber um sinal de frequência $[f]$ 100 Hz.

Resolução

Sabendo que: $T = \frac{1}{f} = \frac{1}{100} = 0,01s$

Se $V = 3 \times 10^8 \text{ ms}^{-1}$

Então, $\lambda = VT = 3 \times 10^6 \text{ m}$

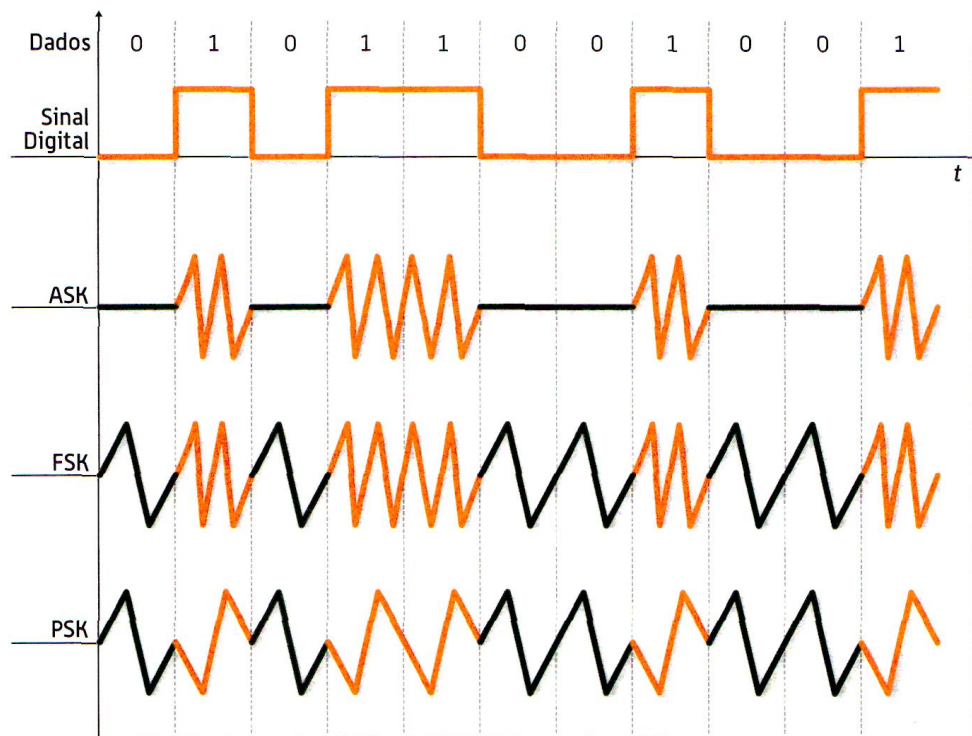
Como o tamanho da antena tem de ser pelo menos um décimo do comprimento de onda tem: $L = \frac{\lambda}{10} = 3 \times 10^5 \text{ m} = 300 \text{ km}$

Como é visível na resolução do exercício anterior, seria impraticável | dispor de uma antena deste tamanho para receber uma frequência do | género. Assim, modulando por exemplo esta frequência na faixa de frequência FM (88 MHz a 108 MHz) com uma antena de apenas um metro já seria possível receber o mesmo sinal.

No âmbito da disciplina de Redes de Comunicação, as modulações mais importantes serão as modulações digitais. Iremos estudar três tipos de modulações digitais, coincidentes com os parâmetros que usualmente variam numa transmissão analógica:

- Modulação em Amplitude (**ASK** - *Amplitude Shift Keying*);
- Modulação em Frequência (**FSK** - *Frequency Shift Keying*);
- Modulação em Fase (**PSK** - *Phase Shift Keying*).

Na **figura seguinte** estão representados os três tipos de modulações para uma determinada sequência de bits a transmitir (dados).



Modulações ASK, FSK e PSK

No caso de ASK, os bits nulos recebem componente nula e os bits de valor 1 recebem uma onda de frequência f . Para a modulação FSK, os bits 0 e 1 alternam respetivamente entre uma onda de frequência f_1 e f_2 . Finalmente, para a modulação PSK sempre que existe uma transição entre 0→1 ou 1→0 existe uma inversão de fase na onda, com sentido contrário à representativa do bit anterior.

GRANDEZAS E MEDIDAS

Para a disciplina de Redes de Comunicação é fundamental conhecer algumas grandezas e medidas. A unidade bit será sem sombra de dúvida a nossa referência na matéria. Saber a quantidade de bits que podemos transferir entre dois pontos por unidade de tempo é essencial para medir a capacidade de um sistema de comunicação. A esta "velocidade" de propagação da informação está associada a capacidade dos equipamentos de rede utilizados, bem como o canal por onde estes são transportados. Cada troço de uma rede tem as suas características específicas, associadas a grandezas e medidas particulares, como se descrevem a seguir.

DECIBEL (DB)

A grandeza decibel é mais conhecida como medida de intensidade do som, porém, também é utilizada para descrever todos os sinais de rede, sejam ondas de voltagem em cobre, impulsos óticos em fibra ou micro-ondas num sistema sem fios.

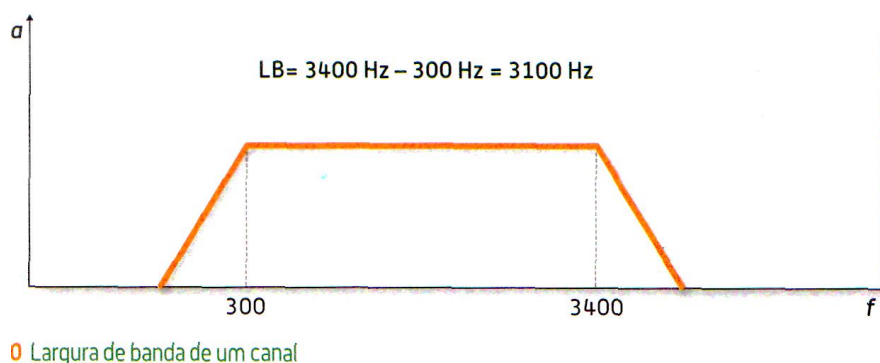
DB mede a perda ou ganho de potência de uma onda. Os decibéis podem ser números negativos, o que representa uma perda na potência (atenuação) da onda ao propagar-se, ou números positivos, o que repre-

senta um ganho na potência se o sinal for amplificado. A sua utilização deve-se sobretudo à simplicidade dos cálculos serem reduzidos a somas e subtrações.

LARGURA DE BANDA

A largura de banda (*bandwidth*) é a medida da capacidade de transmissão de um determinado meio, conexão ou rede, que indica a velocidade a que os dados passam através desse meio, entre dois pontos e num determinado intervalo de tempo.

A largura de banda de um canal é definida como a diferença entre a frequência mais alta e a mais baixa que o canal pode realmente transmitir.



O conceito de largura de banda está associado a dois tipos de sinais diferentes: os sinais digitais e os analógicos.

A unidade básica para descrever a largura de banda é o bit **por** segundo (bit/s). Por exemplo, uma ligação ADSL a 2 Mbit/s indica que podem ser transmitidos 2 Mbit de informação por cada segundo que passe (limite teórico). A largura de banda pode ser comparada a um cano de água. Quanto maior for o diâmetro do cano, maior o caudal de água que poderá passar por ele. Da mesma forma, quanto maior a largura de banda, maior a capacidade de transmissão de informação pelo canal.

| Unidade de largura de banda | Abreviatura | Equivalência |
|-----------------------------|-------------|---|
| Bit por segundo | bps | 1 bps = Unidade básica da Largura de banda |
| Quilobit por segundo | kbps | 1 kbps = 1000 bps |
| Megabit por segundo | Mbps | 1 Mbps = 1000 kbps = 1 000 000 bps |
| Gigabit por segundo | Gbps | 1 Gbps = 1000 Mbps = 1 000 000 kbps = 1 000 000 000 bps |

Unidades de largura de banda digital

Quando os sinais são analógicos, a largura de banda é a diferença entre as frequências ($f_2 - f_1$), como é apresentado na figura seguinte

A unidade de medida da largura de banda para sinais analógicos é o Hertz (Hz), intensidade/tensão (db)

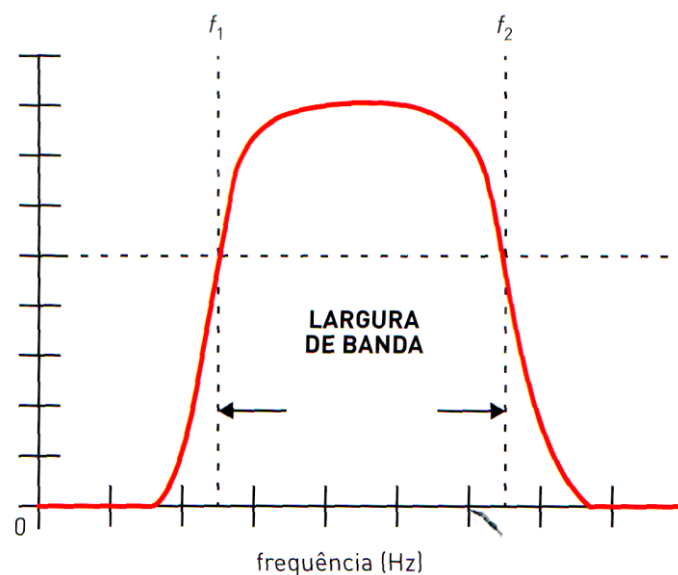


Figura 1.23 Largura de banda - sinal analógico

Vejamos dois exemplos que permitem ilustrar o conceito de largura de banda:

- a) Cano de água: a quantidade de água por unidade de tempo que pode ser escoada por um cano fino é muito menor que aquela debitada por um cano grosso (figura 1.22).
- b) Autoestrada: a quantidade de carros que passam pelas portagens num determinado intervalo de tempo numa autoestrada com duas faixas é menor que a verificada numa autoestrada com quatro faixas (figuras 1.24 e 1.25).

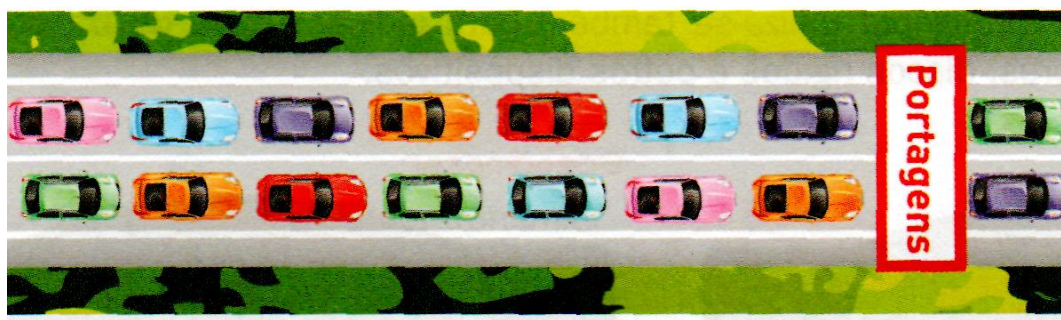
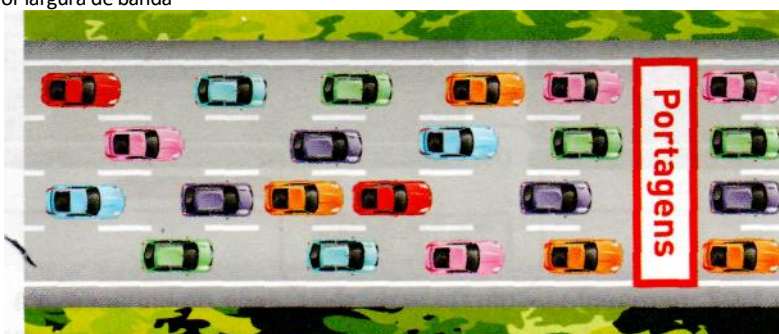


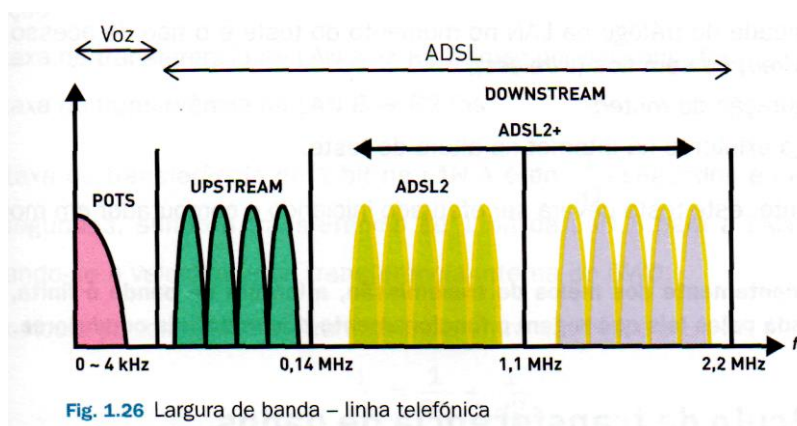
Fig. 1.24 Menor largura de banda



Maior largura de banda

A largura de banda é responsável pela limitação da taxa de transmissão de dados. Por exemplo, a ligação Dialup de 56 k é limitada pela largura de banda da linha telefónica (0-4 kHz).

A figura 1.26 mostra o espectro de frequência de um sinal ADSL.



THROUGHPUT

No momento em que contratamos um serviço de Internet a um ISP (*Internet Service Provider*) é-nos fornecida uma certa largura de banda. No entanto, apesar de se contratar, por exemplo, 2 Mbit/s de largura de banda nunca se dispõe realmente desse valor. O verdadeiro valor chama--se *throughput*, que pode ser traduzido como a taxa de transferência efetiva de um sistema de transmissão ou ainda como a quantidade de dados transferidos por unidade de tempo. Existem dois fatores que podem influenciar o *throughput*:

- **A frequência máxima de transmissão** (limitada pelo tipo de canal utilizado). Imagine que queremos fazer download de um ficheiro que se encontra num servidor em França. Desde lá até ao nosso PC passamos por vários tipos de infraestruturas de rede contendo vários tipos de equipamentos (uns mais rápidos, outros mais lentos). Essas infraestruturas poderão ser cabos de cobre, fibra ótica ou mesmo comunicação sem fios. Cada um deles, dependendo do meio que utiliza para propagar a informação (cobre, ar, fibra), conta com diferentes frequências máximas de transmissão, que por sua vez influencia a quantidade de dados transferidos por unidade de tempo (*throughput*). Quando a informação chega finalmente ao nosso PC, já passou por várias redes, inclusive por algumas bem mais "lentas" do que aquela fornecida pelo nosso ISP.
- **A taxa de erro do canal.** Genericamente, quando se utilizam cabos de cobre para a transmissão, a taxa de erros é bastante elevada. Assim, é necessário adicionar cabeçalhos de controlo de erros à informação que está a ser transmitida. Estes são, para todos os efeitos, mais informação adicionada ao que pretendemos transmitir, logo levará mais tempo a realizar-se a transferência. Por outro lado, os cabeçalhos serão alvo de verificação de erros por parte do recetor o que provoca atraso na transferência. Os problemas aqui citados são responsáveis pela redução da largura efetiva do canal (*throughput*)

BIT RATE

Bit Rate significa taxa de bits. Bit Rate (às vezes escrito como bitrate) Data Rate pode ser visto como uma

analogia a um conta-quilómetros de um automóvel. A velocidade que o conta-quilómetros marcar é a velocidade naquele instante de tempo do carro. Da mesma forma, o bitrate é -- velocidade com que os bits são convertidos ou processados por unidade de tempo. Por vezes, o bitrate é utilizado como grandeza de medida para codificar ficheiros multimédia. São os casos dos ficheiros *Mp3*, *Divx*, *RMvb*, etc.

TÉCNICAS DE CODIFICAÇÃO

Na transmissão de dados é fundamental transmitir a informação sem erros, por isso a codificação tem como principal objetivo preservar o sincronismo do relógio entre o emissor e o recetor. Quando transmitimos informação, independentemente do canal utilizado, esta está sujeita a atrasos, ruído e erros introduzidos pelo canal ou pelos equipamentos de rede por onde passa. Os códigos de linha foram criados para ajudar a manter a integridade dos dados ao longo do seu percurso. Em geral, os códigos de linha devem ter em conta certos aspetos, como a largura de banda que utilizam, a imunidade a erros e ruídos, o tempo de bit (*Duty Cycle*), a possibilidade de recuperação do relógio de sincronismo (CLK) e a existência de componente contínua nula (transformadores ao longo do canal que bloqueiam o sinal contínuo não nulo). Existem vários tipos de códigos de linha, como será possível verificar de seguida, cada um apresentando vantagens e desvantagens relativamente aos diferentes sistemas de comunicação onde são aplicados. Em cada código de linha que se segue são resolvidos exercícios para ajudar à compreensão desta temática.

NRZ

O código de linha do tipo *Non Return Zero* indica que o sinal não necessita obrigatoriamente de ir a zero entre transições de bit. Tem *Duty Cycle* de 100% (o impulso prolonga-se durante todo o bit). Existem três tipos de codificação NRZ.

NRZ UNIPOLAR

Este tipo de codificação é a mais simples (a sua única vantagem). Apresenta alguns problemas, como por exemplo, a componente DC não nula e as longas sequências de 0's ou 1's determinam que facilmente perca sincronismo. Os limites da onda estão sempre entre 0 e 1 e tomam o valor 1 quando o bit a codificar é 1 e 0 quando o bit a codificar é 0. É utilizado para gravação digital em suportes magnéticos.

NRZ POLAR

Este tipo de codificação apresenta as mesmas vantagens e desvantagens do anterior. Os limites da onda neste tipo de codificação estão entre -1 e 1. A onda codificada toma o valor 1 quando o bit a codificar ele toma o valor -1 quando o bit a codificar é 0. Também é usado para gravação digital em suportes magnéticos.

NRZ BIPOLAR (AMI)

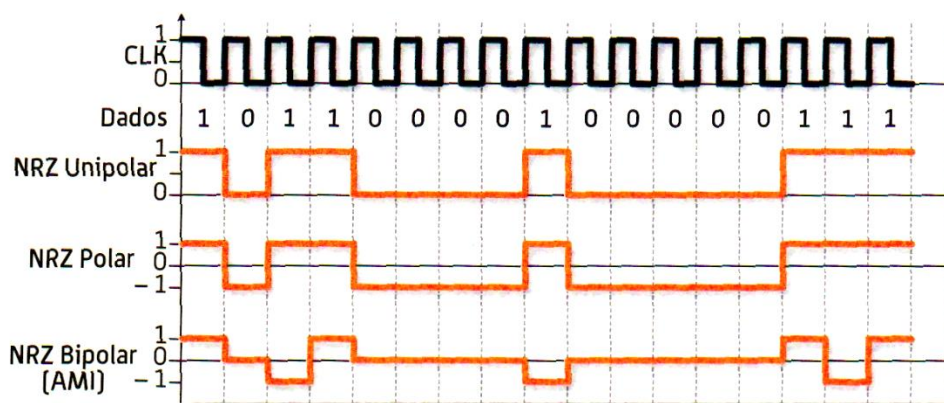
Este tipo de codificação resolve o problema relativo à componente DC mas sofre igualmente de perda de

sincronismo com facilidade. Os limites da onda neste tipo de codificação estão entre -1, 0 e 1. Toma o valor 0 quando o bit a codificar é 0 e toma o valor 1 e -1 alternadamente quando o bit a codificar é 1. É utilizado nas interfaces **RDIS**.

RDIS ou **rede digital com integração de serviços**, que tal como o nome indica, para além de voz permite a integração de serviços (dados) pela mesma interface. Usa a rede telefónica para operar com acesso básico 2B+D onde B representa um canal de taxa igual a 64 Kbit/s para voz e dados e um canal D com 15 Kbit/s para sinalização.

EXERCÍCIO RESOLVIDO

Codifique a seguinte sequência de bits 10110000100000111 com os seguintes códigos de linha: NRZ unipolar, NRZ polar e NRZ Bipolar. Nota: acompanhe o exercício com o modo de funcionamento de cada código descrito anteriormente.



Códigos de linha NRZ

RZ

O código de linha do tipo *Return Zero* indica que, em cada transição, metade do bit o sinal vai a zero. Diz-se por isso que tem um *Duty Cycle* de 50% e utiliza o dobro da largura de banda em relação aos códigos NRZ. Existem três tipos de codificações RZ.

RZ UNIPOLAR

Este tipo de codificação apresenta as mesmas vantagens e desvantagens do NRZ unipolar com a agravante de que utiliza, como já foi referido, o dobro da largura de banda. Os limites da onda estão sempre entre 0 e 1 e tomam o valor 1 quando o bit a codificar é 1 e 0 quando o bit a codificar é 0. No entanto, só permanecem nesses valores metade do tempo do bit (*Duty Cycle* = 50%). Na outra metade, tomam sempre o valor 0. É usado nas mesmas aplicações que NRZ unipolar.

RZ POLAR

Este tipo de codificação apresenta as mesmas vantagens e desvantagens do NRZ polar (e o dobro da largura

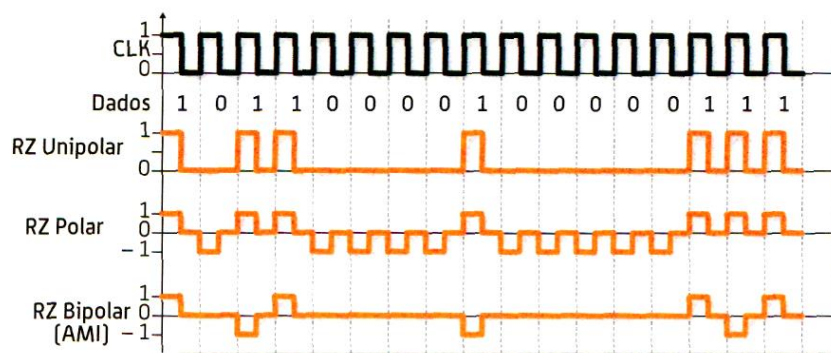
de banda). Os limites da onda neste tipo de codificação estão entre -1 e 1. A onda toma o valor 1 quando o bit a codificar ele toma o valor -1 quando o bit a codificar é 0. No entanto, mais uma vez, só permanecem nesses valores metade do tempo do bit (*Duty Cycle* = 50%). Na outra metade tomam sempre o valor 0. É usado nas mesmas aplicações que NRZ polar.

RZ BIPOLAR (AMI)

Este tipo de codificação apresenta as mesmas vantagens e desvantagens do NRZ Bipolar (e o dobro da largura de banda). Os limites da onda neste tipo de codificação estão entre -1, 0 e 1. Toma o valor 0 quando o bit a codificar é 0 e toma o valor 1 e -1 alternadamente quando o bit a codificar é 1. Contudo, só permanecem nesses valores metade do tempo do bit (*Duty Cycle* = 50%). Na outra metade tomam sempre o valor 0. É usado nas mesmas aplicações que NRZ bipolar.

EXERCÍCIO RESOLVIDO

Codifique a seguinte sequência de bits 10110000100000111 com os seguintes códigos de linha: RZ unipolar, RZ polar e RZ bipolar. Nota: acompanhe o exercício com o modo de funcionamento de cada código descrito anteriormente.



Códigos de linha RZ

TÉCNICAS DE DETECÇÃO E CORREÇÃO DE ERROS EM TRANSMISSÕES DIGITAIS

Seja qual o meio em que comunicamos podem ocorrer situações que dificultam a correta transmissão da mensagem. Quando estamos em ambientes ruidosos temos dificuldade em ouvir alguém que fale connosco, nas transmissões de dados, fenómenos como o ruído e as interferências também ocorrem, podendo deturpar a mensagem original. Devido a este problema são aplicados códigos de detecção e correção de erros às transmissões.

DETEÇÃO DE ERROS

Vamos descrever três códigos detetores de erros que são os mais frequentemente utilizados em redes de comunicação: verificação de paridade, *checksum* e CRC.

VERIFICAÇÃO DE PARIDADE

Este é um dos métodos mais utilizados para a deteção de erros. O bit de paridade indica o número de bits 1 presentes num carácter (Byte). Assim, diz-se que a paridade é par se tiver um número par de 1's e ímpar caso tenha número ímpar de 1's. Como vimos anteriormente, no caso das tramas síncronas o último bit do byte, se não contiver dados, é utilizado para verificação de paridade. Assim, este assume o bit 0 quando temos paridade par e 1 quando temos paridade ímpar. Vejamos os exemplos:

- 11001100 - a mensagem está correta. O último bit é zero indicando que o número de 1's que o precede é par (4 uns).
- 10101011 - a mensagem está errada. O byte teria assim de ser retransmitido visto o bit de paridade dizer que o número de 1's é ímpar e, no entanto, é par (4 uns).

Contudo poderão existir erros e o bit de paridade indicar que a transmissão foi feita sem erros. Vejamos o exemplo seguinte:

- 10111101 - o bit de paridade indica que existe número ímpar de 1's na transmissão, o que está correto. No entanto, imaginemos que sabemos que os dois bits 1's que estão sublinhados foram alvos de erro. Então, o verdadeiro valor destes bits seria zero. Vejamos o bloco de bits sem erro.
- 10011001 - como podemos verificar o bit de paridade indica que o número de 1 presente no bloco transmitido é ímpar, o que mais uma vez é verdade apesar de termos corrigido os bits que estavam anteriormente errados. Conclusão, sempre que o número de bits errados for par não é detetado erro, segundo esta abordagem.

CHECKSUMS

São técnicas utilizadas para detetar erros principalmente na Internet e denominam-se somas de verificação. Esta verificação é usada ao nível de transporte e baseia-se na soma do conteúdo do segmento que é colocado numa posição da trama UDP, no lado do emissor. No recetor, há lugar novamente à soma do segmento. Se a soma de checksums (normal e complemento para 1) resultarem apenas 1's, podemos inferir que "não" houve erro na transmissão, caso contrário, existiu erro na transmissão. Esses erros são assinalados nas posições que da soma de checksums resultem zeros. Os erros podem ocorrer no segmento ou no próprio código detetor de erros.

| No emissor | No recetor |
|---|---|
| <ul style="list-style-type: none">– Trata o conteúdo do segmento como uma sequência de inteiros de 16-bits;– Checksum: soma (em complemento para 1) do conteúdo do segmento;– Emissor coloca o valor calculado no campo <i>checksum</i> do datagrama UDP. | <ul style="list-style-type: none">– Calcula o checksum do segmento recebido;– Verifica se a soma dos checksums resultam 1's.<ul style="list-style-type: none">○ NÃO-erro detetado○ SIM-não detetou erro... embora possa existir erro mesmo assim. |

Resumo do funcionamento do código detetor de erros checksum

Para que se compreenda melhor o que anteriormente foi referido resolve-se de seguida um exercício.

EXERCÍCIO RESOLVIDO

Indique qual o valor em binário a juntar a 2 byte (00111101 e 00001101) de informação para que estes sejam transmitidos com um código detetor de erros do tipo *checksum*. Faça a verificação no recetor.

O primeiro passo será do lado do recetor, este deverá proceder à soma da informação a enviar, para assim ser calculado o *checksum* a adicionar à transmissão.

$$\begin{array}{r} 00111101 \\ 00001101 \\ \hline +01001010 \end{array}$$

Como a soma tem de ser em complemento para 1 terá de inverter a sequência resultante da soma normal (zeros passam a uns e vice-versa. Obteremos então, a sequência de *checksum* invertido seguinte:

Checksum Invertido: **10110101**

Os dados enviados serão então: 00111101 00001101 10110101, ou seja, os 2 byte iniciais mais a sequência de *checksum* invertida.

Para verificar se ocorreram erros durante a transmissão, no recetor, teremos de voltar a somar os 2 byte de dados enviados e somar ao *checksum* invertido. Assim, considerando que não existiram erros, o *checksum* seria de novo o calculado anteriormente, ou seja, 01001010. Somando ao *checksum* invertido que foi adicionado no emissor vem:

$$\begin{array}{r} 10110101 \text{ checksum invertido (emissor)} \\ 01001010 \text{ checksum recetor} \\ \hline +11111111 \end{array}$$

Como todos os bits resultantes desta soma são 1 então não existiu erro na transmissão. No caso de algum desses bits ser diferente de 1, então nessa posição (de qualquer um dos bytes ou mesmo do código de *checksum*) teria ocorrido erro.

Este método apresenta, à semelhança do anterior, algumas falhas. Poderá não se detetar erros:

- se os bits não estiverem ordenados;
- se tiverem sido inseridos bits nulos;
- ocorram múltiplos erros que se anulem entre si.

CORREÇÃO DE ERROS

Anteriormente identificámos formas de detectar os erros. Porém, esses erros apenas eram detetados e não corrigidos. Geralmente quando um erro é encontrado toda a informação terá de ser retransmitida. Esta, já por si, é uma forma de "corrigir" erros - a retransmissão. A técnica utilizada chama-se ARQ - *Automatic Repeat Request* baseia-se em confirmações positivas (ACK) e confirmações negativas por parte do recetor (NACK).

As tramas de dados não aceites pelo recetor são descartadas e terão de ser retransmitidas. As versões mais utilizadas de ARQ são o *Stop and Wait ARQ*, o *Go-back-N ARQ* e o *Selective Reject ARQ*. No entanto, existem formas de corrigir erros sem que seja necessária a retransmissão da informação. Um exemplo disso é o código de Hamming que permite detetar e corrigir erros, sem que seja sempre necessária a retransmissão. Este código foi desenvolvido por Richard Wesley Hamming (1915-1998), um matemático americano que contribuiu bastante para a área das telecomunicações. O seu código é utilizado quando a importância da mensagem chegar ao destino é maior do que a de chegar rapidamente (ex.: mensagens enviadas para a sonda que está em Marte). Este código acrescenta à mensagem a transmitir informação redundante. A distância de Hamming será calculada através da diferença entre os bits da mensagem enviada e recebida. Por exemplo:

11110011

101110001

A distância de Hamming (m) é igual a 2, visto existirem dois bits diferentes entre as duas sequências.

Dependendo desta distância " m " o código de Hamming permite:

- **detetar** até $m-1$ bits errados;
- **corrigir** até $(m-1)/2$ (arredondado para baixo) bits errados.

Assim, se a distância de Hamming for:

$$m = 5$$

- **Detetam-se** até 4 bits errados e corrigem-se até 2 bits errados.

TÉCNICAS DE COMPRESSÃO DE DADOS

A compressão de ficheiros está na ordem do dia. Cada vez mais se torna importante aceder às "coisas" rapidamente, mas também com a melhor qualidade possível. Todos os dias ouvimos falar de ficheiros Mp3, DivX, Rmvp e muitos outros. Estes são exemplos de ficheiros comprimidos que dependendo dos parâmetros e técnicas de compressão utilizadas apresentam melhor ou pior relação espaço/qualidade. Desta forma podemos dizer que a compressão de dados permite:

- reduzir o espaço ocupado pelos ficheiros em disco;
- reduzir o tempo de transferência de ficheiros.

A compressão não é mais que a remoção do que é redundante e/ou do que é irrelevante no conjunto da informação original.

Mas afinal como é possível comprimir informação? Podemos fazê-lo aplicando algoritmos, com e sem perdas. Os pontos seguintes descrevem em pormenor cada uma dessas técnicas.

COMPRESSÃO COM PERDAS

A compressão com perdas tira partido da redundância e da irrelevância. As perdas são irreversíveis. Na descompressão não é possível recuperar o que foi eliminado durante a compressão. A compressão com perdas é usada para ficheiros multimédia, por exemplo, vídeo (MPEG), música (Mp3) e imagem (JPEG). No

caso particular dos ficheiros Mp3 é possível obter um ficheiro com a mesma qualidade que o ficheiro original com apenas 1/10 do tamanho. Este tipo de compressão, como indicado acima, tira partido da redundância e da irrelevância, tendo o segundo um papel de grande importância quando comprimimos um ficheiro para Mp3. A verdade é que o ser humano, em média, apenas é capaz de ouvir as frequências no intervalo [20Hz, 20KHz] - limiar de audição. Então porque não eliminar todas as frequências que não se encontrem neste intervalo? É exatamente este o princípio que é aplicado à compressão de ficheiros Mp3 e que lhes permite manter a qualidade apesar do tamanho reduzido.

Quando falamos de compressão de vídeo, eliminar a redundância é a palavra-chave. Sabendo que um vídeo é composto por imagens que são mostradas sequencialmente, comparam-se imagens seguidas mantendo a informação que não mudou de uma para a outra codificando apenas os píxeis relativos à mudança (macrobloco).

A compressão com perdas é uma das técnicas mais utilizadas para comprimir ficheiros multimédia.

COMPRESSÃO SEM PERDAS

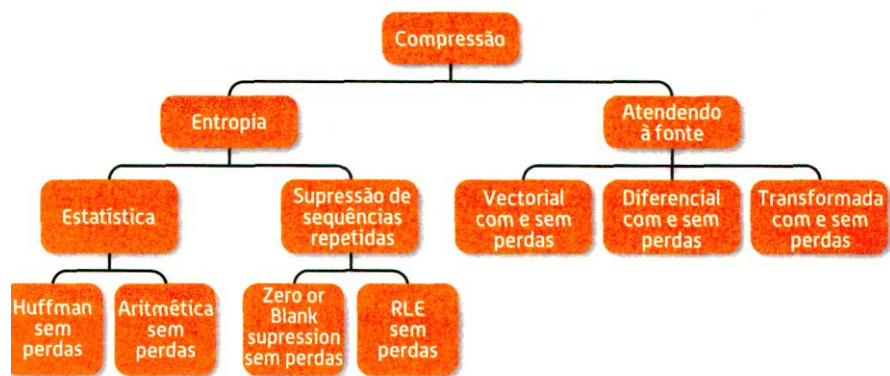
A compressão sem perdas tira partido apenas da redundância (informação a mais da qual se pode prescindir sem que existam perdas). A informação é recuperada sem qualquer alteração após o processo de descompressão. Este processo é utilizado para compressão de texto e em aplicações onde a informação seja muito importante (transações bancárias, informação médica, etc). Os ficheiros associados a este tipo de compressão são o zip, rar, arj entre outros.

É muito usual a compressão de ficheiros de texto. Claramente esta compressão não pode ser com perdas, ou perderíamos parte na nossa informação. Aplica-se sim um algoritmo sem perdas que irá analisar o texto e verificar as redundâncias. Entenda-se redundância como a frequência com que uma determinada palavra aparece no texto. Após esta análise, substituem-se as palavras por símbolos que irão permitir ocupar um espaço menor em disco. O processo pode ser invertido através de correspondência entre símbolos e palavras na descompressão (tabela de correspondência).

NATUREZA DOS DADOS

O processo de compressão pode ser realizado com conhecimento ou não da natureza dos dados a comprimir. Chama-se compressão por entropia quando esta não tem em conta a natureza dos dados a comprimir. Por outro lado, quando é tido em conta a natureza dos dados a comprimir designa-se compressão atendendo à fonte. No primeiro caso, os algoritmos são sempre sem perdas, enquanto no segundo são aplicados tanto a algoritmos com perdas como sem perdas. Esta diferença é evidente quando tentamos comprimir por exemplo um ficheiro de música no formato Wav em ficheiro Zip. Não resultará deste processo qualquer compressão, já que este algoritmo não tem em conta o tipo de dados que está a comprimir aplicando sempre a mesma técnica independentemente do tipo de ficheiro.

De seguida, encontra-se um resumo sobre a compressão de dados



A INFORMAÇÃO

O QUE É A INFORMAÇÃO

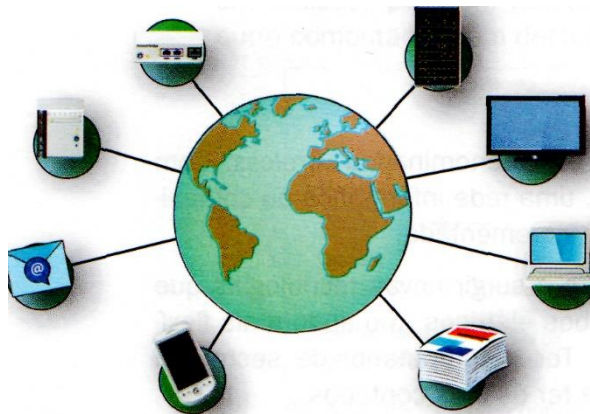
Vivemos num mundo que se encontra em constante transformação e expansão, onde estar informado se tornou numa necessidade quase tão existencial como respirar. Estar informado e ter acesso rápido a uma determinada informação pode estabelecer a diferença entre o sucesso e o fracasso, a sorte e o azar.

Desde sempre a Humanidade sentiu necessidade de se informar e de aprender, ou seja, de adquirir formação. Já para os latinos, a **informação**, de *informatione*, era a ação de modelar, fabrico, construção, obra, planta, desenho, formação e forma.

Hoje em dia, a palavra "informação" remete-nos de imediato para os jornais, notícias, televisão e poucos são os que pensam em livros, pesquisa ou formação.

De facto, pensa-se logo em comunicação e torna-se difícil estabelecer uma distinção entre os dois conceitos. A comunicação põe em comum, reúne, mistura e divulga a informação. Nas novas tecnologias, esta comunicação da informação (ato ou efeito de emitir ou receber mensagens) é feita por meios mais modernos, tais como máquinas de fax, satélites, câmaras de vídeo, leitores de CD, impressoras, computadores pessoais e telefones, entre outros menos divulgados.

A informação é, então, o "termo que designa o conteúdo de tudo aquilo que trocamos com o mundo exterior e que faz com que nos ajustemos a ele de forma perceptível" (Wiener).



QUALIDADE DA INFORMAÇÃO

Encontramo-nos num mundo em que se sente uma necessidade cada vez maior de informar e ser informado, mas em que, por outro lado, também somos invadidos por excesso de informação, tanta e tão variada que nos é impossível absorvê-la e tratá-la na sua totalidade.

Dado a importância da informação nos dias de hoje. Espera-se que esta seja, no mínimo, **exata** (ou seja, isenta de erros, verdadeira), oportuna (ou seja, atual, recente) e **clara** (ou seja, compreensível, direta).

No entanto, a informação é uma mercadoria e, como tal, tem um custo de venda e um custo de compra; devido a isto, a informação é muitas vezes tanto ou mais **quantitativa** do que **qualitativa**. Os órgãos de comunicação social vivem da notícia! Atualmente, a informação é empírica e de certo modo demagógica, na medida em que procura dar ao público tudo o que ele quer, sem preocupações de qualidade no tratamento da informação ou veracidade comprovada do conteúdo informado.

Tratamento da informação

Ao longo da História, a informação foi tratada com meios e métodos que estavam em conformidade com as épocas e o estado de desenvolvimento tecnológico da sociedade.

No início, sendo a informação tratada manualmente, era normal que na sua transmissão surgissem vários erros (devido a más interpretações, desatenções ou cansaço físico) e, com eles, os consequentes inconvenientes. Também a velocidade a que um ser humano consegue trabalhar fica muito aquém das necessidades atuais exigidas no tratamento da informação. Necessitava-se então de um instrumento mais fiável e rápido, embora o tratamento manual de dados ainda hoje se use em pequenas empresas, com uma capacidade financeira e uma quantidade de informação reduzidas.

A quantidade de informação a transmitir era cada vez maior e mais complexa e por isso tornou-se necessário estabelecer uma certa ordem e organização da mesma, para que o acesso a um determinado tipo de informação fosse mais rápido e acessível. Com a Revolução Industrial foi-se ao encontro dessa necessidade. Começaram-se a desenvolver máquinas de processamento de dados com base num funcionamento mecânico e, posteriormente, com base num funcionamento **eletrónico**, permitindo, então, aumentar a **exatidão e a velocidade de transmissão** de informação.

Numa sociedade em que o tempo escasseia e em que ser o primeiro a obter e a tratar a informação se torna quase imperativo, fomos obrigados a desenvolver e a usar ferramentas de transmissão de informação cada vez mais sofisticadas (quase instantânea) em grandes quantidades e a elevadas velocidades. Como nenhuma outra ferramenta conhecida até aos dias de hoje, o computador atual serve este fim na perfeição: é veloz, fiável e com uma enorme capacidade de armazenamento. Mas de pouco nos serve uma ferramenta tão capaz se não soubermos tirar partido dela. Teremos de aprender a fornecer ordens corretas e coerentes, através de um programa de computador, para que este, depois, nos forneça a informação pretendida.

A informação constante num computador pode ser tratada com base em dois processos distintos:

- ⇨ o **tratamento em *batch***, ou seja, os dados são recebidos num determinado período e agrupados em **lotes**, para posteriormente serem processados em conjunto;
- ⇨ o **tratamento em tempo real**, ou seja, os dados não necessitam de esperar pela criação de um lote. Os dados são processados no momento real em que são recebidos.

Essa mesma informação encontra-se normalmente classificada em dois tipos de ficheiros:

- ⇨ os **ficheiros de dados (*data files*)** - os que contêm dados, ou seja, a base para o tratamento da informação e sobre a qual o computador efetua as operações necessárias à tarefa em questão (o processamento de dados);
- ⇨ e os **ficheiros de programas (*program files*)** - os que manipulam os dados.

Dentro de cada uma destas categorias existem ainda diferentes tipos de ficheiros, que armazenam vários tipos de informação.

Tipos de informação

Os tipos de informação a que se pode ter acesso através de um computador são:

- ↪ em forma de texto, gráficos (imagens gráficas), animações e ficheiros digitais de *media* [sons (áudio), vídeo e realidade virtual].

A informação a que depois se tem acesso poderá ser:

- ↪ uma **informação direta**: a que se estabelece entre duas pessoas (emissor e recetor) ou entre uma pessoa (emissor) e um grupo (recetor). Exemplos: conferência, *talk*, conversação interpessoal;
- ↪ uma **informação escrita**: a que se estabelece entre pessoas ou grupos através de um meio de comunicação escrita. Pode ser direta (*e-mail*, fax) ou indireta (imprensa, Internet);
- ↪ uma **informação icónica**: a que se serve de imagens (fixas ou em movimento) para a emissão de mensagens;
- ↪ uma **informação de massas**: forma de comunicação dirigida a uma ampla faixa de público anónimo, disperso e heterogéneo, atingindo simultaneamente (ou a breve trecho) uma grande audiência, graças à utilização dos meios de comunicação de massa (Internet, televisão, rádio, jornal);
- ↪ ou uma **informação múltipla**: tipo de informação direta que se dirige, por escrito, a uma pluralidade de recetores indiferenciados (uma circular, aviso de vírus).

ESTÁDIOS DE INFORMAÇÃO

Há muito tempo que o ser humano teve noção das vantagens de se manter informado e de informar os outros. Por isso, foi desenvolvendo múltiplas formas de transmitir esses conhecimentos, passando por vários estádios até chegar aos dias de hoje.

1.º estádio - num período pré-histórico - informação através de sinais de fumo; a linguagem primária; pinturas rupestres; pegadas.

2.º estádio - até à segunda metade do século XIX, passando pela expansão da imprensa - informação através da linguagem falada ou escrita (jornais, revistas, livros) e através da expressão artística.

3.º estádio - da segunda metade do século XIX até finais do século XIX, por meio da divulgação da imagem e som -informação transmitida devido ao surgimento da fotografia, telégrafo, fotogravura, ilustrações, telefone, fonógrafo, gramofone, transmissões radiotelegráficas, apresentação do cinematógrafo, emissões de rádio.

4.º estádio - do início do século XX até aos anos 70 -com a divulgação em massa da informação, através do aparecimento da televisão, do cinema sonoro, das fotografias a cor, do satélite de comunicação (cujo primeiro foi o TELSTAR), do satélite Intelsat (que possibilita a comunicação telefónica, telegráfica, radiofónica e televisiva) e da chegada do Homem à Lua.

5.º estágio - a partir dos anos 70 até aos dias de hoje - com a aplicação da eletrónica à composição de impressos, a revolução tecnológica nas artes gráficas, a comercialização maciça de videogravadores, as redes de telemática e de bancos de dados, os telefones portáteis, os computadores, a Internet.

INFORMAÇÃO DIGITAL

Quando comunicamos com outras pessoas, utilizamos códigos que nos são familiares, como é o caso da linguagem escrita, falada ou gestual, entre outras. No caso dos computadores, também existe um processo semelhante ao humano. O computador trata a informação internamente, mas de um modo codificado, o que torna este processo muito diferente do utilizado pelo ser humano.

Podemos então questionar-nos de que modo o ser humano pode interagir com o computador e vice-versa.

Na realidade, o computador não entende os símbolos que constituem a linguagem humana (ex.: letras e números). Para tal, foi necessário traduzir e codificar os nossos símbolos numa linguagem própria da máquina, utilizando circuitos eletrónicos. Na prática, estes circuitos funcionam como um sistema complexo de interruptores que podem ser ligados e desligados a uma grande cadência, sendo controlados por uma unidade de controlo, que deixa passar ou não corrente elétrica para o circuito.

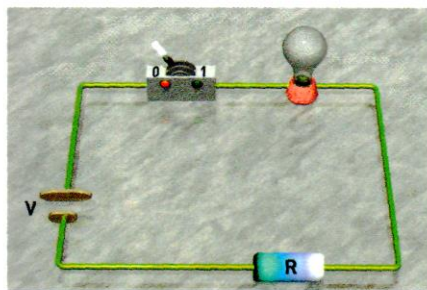


Fig. 1.13 Funcionamento de um interruptor a controlar uma lâmpada
Lâmpada apagada "0 ou OFF"

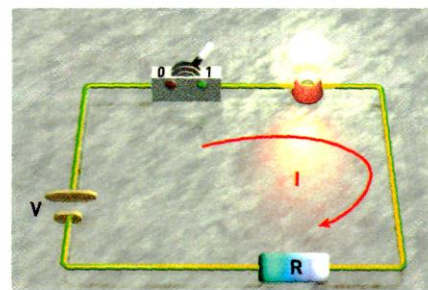
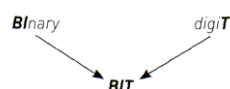


Fig. 1.14 Funcionamento de um interruptor a controlar uma lâmpada
Lâmpada acesa "1 ou ON"

Analisando os exemplos das figuras 1.13 e 1.14, o computador só é capaz, num dado instante, de distinguir uma das duas situações possíveis: a lâmpada está desligada "OFF" - não passa corrente no circuito - ou a lâmpada está ligada "ON" - passa corrente no circuito.

Dado o computador ser apenas capaz de distinguir, num determinado momento, uma de duas situações, usa um código que é baseado em **apenas dois** símbolos, embora permita representar todos os símbolos necessários. Este código, por ser baseado apenas em dois símbolos, designa-se por código **binário**.

Os símbolos que compõem o código são representados pelos algarismos 0 e 1, aos quais também se pode chamar *bit*. O termo *bit* foi introduzido por John Tukey, um estatístico americano e um dos primeiros cientistas de computadores. Usou o termo pela primeira vez em 1946, como abreviatura para dígito binário (*binary digit*), a unidade mais pequena de informação num computador.



CLASSIFICAÇÃO DAS REDES DE COMPUTADORES

As redes de computadores podem ser classificadas tendo em conta a sua formas de distribuição geográfica, o papel do computador na rede, ou seja, a forma como os computadores trocam informações entre si e a hierarquia. O processo de transmissão de dados; via rede começa pelo nível físico e termina ao nível das aplicações dos utilizadores.

CLASSIFICAÇÃO DAS REDES QUANTO À EXTENSÃO GEOGRÁFICA

Neste âmbito, as redes são classificadas quanto ao alcance das mesmas, sendo que diversas classificações são propostas como forma de caracterização destes tipos de redes, conforme os tópicos a seguir:

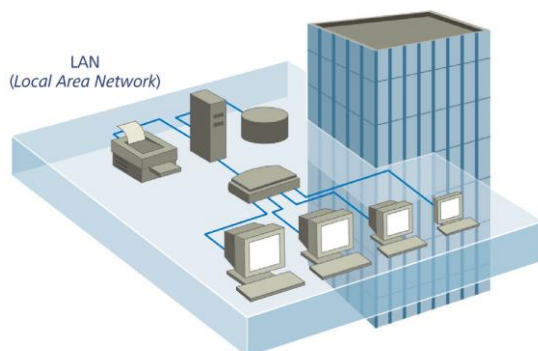
Uma PAN (*Personal Area Network*) ou Rede de Área Pessoal, constitui-se de uma rede de computadores formada por dispositivos muito próximos uns dos outros. Como exemplo deste tipo de rede, pode-se citar dois *dispositivos* numa sala a trocar informações entre si e ligados a uma impressora. Redes formadas por dispositivos Bluetooth são exemplos de uma PAN.



LAN

Uma LAN (*Local Area Network*), também conhecida como rede local de computadores, corresponde a uma rede que possui uma “cobertura limitada” quanto a extensão geográfica que pode atuar.

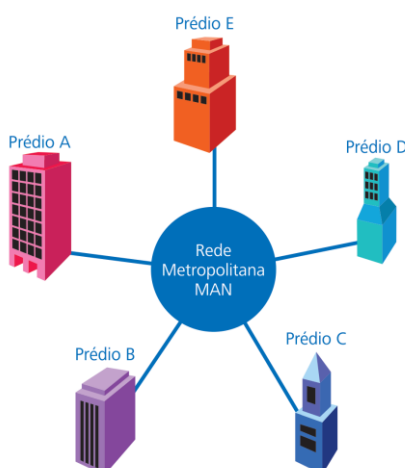
Este tipo de rede é geralmente composto por computadores conectados entre si, através de dispositivos tecnológicos (placas de redes, *switch*, *hub*, entre outros), possibilitando a partilha de recursos e a troca de informações.



Uma rede local de computadores é utilizada com frequência para conectar computadores em rede, servidores, dispositivos eletrônicos diversos (*tablets*, portáteis, *pc's*, etc.). A sua limitação geográfica faz com que as LAN's sejam utilizadas em casas, escritórios, escolas, empresas, entre outros meios locais.

MAN

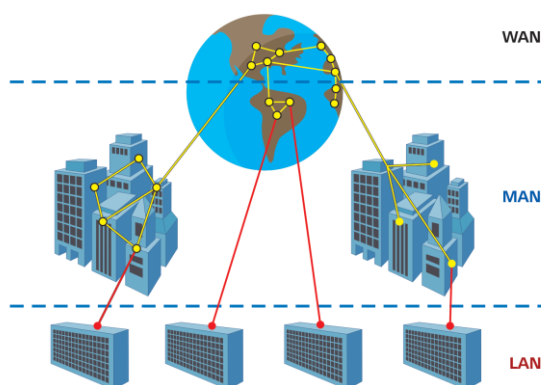
Uma MAN (*Metropolitan Area Network*) rede de área metropolitana, corresponde a uma rede de computadores que compreende um espaço de média dimensão (região, cidade, campus, entre outros). Geralmente uma MAN está associada a interligação de várias LAN's e é considerada uma parte menor de uma WAN (que será descrita no próximo item).



Um exemplo de MAN são as redes ISP (*Internet Service Provider*) que em português significa “fornecedor de serviço de internet”. Um ISP nada mais é do que uma empresa (fornecedor) que fornece acesso à internet e outros serviços como: contas de *e-mail*, hospedagem de *sites*, entre outros, mediante o pagamento de uma mensalidade ou taxa. As formas de conexão a esta rede podem ser através de uma linha telefónica (*dial-up*), ou uma conexão de banda larga (*wireless*, cabo ou DSL). As redes ISPs são exemplos clássicos de MAN.

WAN

Uma WAN (*Wide Area Network*) ou rede de longa distância, corresponde a uma rede de computadores que abrange uma grande área geográfica, como por exemplo um país, continente, entre outros. As WAN's permitem a comunicação a longa distância, interligando redes dentro de uma grande região geográfica.



OUTRAS CLASSIFICAÇÕES QUANTO A EXTENSÃO GEOGRÁFICA

Uma série de outras nomenclaturas são utilizadas para descrever outros tipos de redes, quanto a extensão geográfica que as mesmas atuam. A seguir é possível conhecer algumas:

- ⇒ **WMAN** – rede de área metropolitana sem fio, destina-se principalmente a operadores de telecomunicações.
- ⇒ **WWAN** – rede de longa distância sem-fio, são comumente utilizadas para criação de redes de transmissão celular.
- ⇒ **RAN** – considerada uma subcategoria de uma MAN, uma RAN (*Regional Area Network*), corresponde a uma rede de computadores de uma região geográfica específica.
- ⇒ **CAN** – uma CAN (*Campus Area Network*) corresponde a uma rede de computadores formada por computadores dispostos em edifícios, prédios, campus, entre outros (MENDES, 2007).

CLASSIFICAÇÃO DE REDES QUANTO À HIERARQUIA

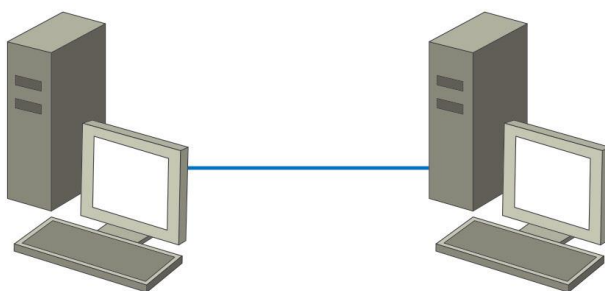
A classificação das redes de computadores quanto a hierarquia refere-se ao modo como os computadores dentro de uma rede se comunicam. Entre os principais tipos de classificação quanto a hierarquia, estão as redes **ponto-a-ponto** e as redes **cliente-servidor**, que veremos a seguir.

REDES PONTO-A-PONTO

Uma rede ponto-a-ponto normalmente é utilizada em pequenas redes. Neste tipo de rede os computadores trocam informações entre si, compartilhando arquivos e recursos. Uma rede do tipo ponto-a-ponto possui algumas características pontuais:

- ⇒ É utilizada em pequenas redes.
- ⇒ São de implementação fácil e de baixo custo.
- ⇒ Possuem pouca segurança.
- ⇒ Apresentam um sistema de cabeamento simples.

Ao citarmos uma vantagem e uma desvantagem deste tipo de rede, podemos considerar como ponto positivo o baixo custo para implementar uma rede do tipo ponto-a-ponto, onde todos os computadores podem conectar diretamente todos os demais computadores e seus recursos partilhados. Um ponto negativo neste tipo de rede está relacionado a baixa segurança que este modelo proporciona.



REDES CLIENTE-SERVIDOR

Uma rede de computadores do tipo cliente-servidor possui um ou mais servidores, responsáveis por prover serviços de rede aos demais computadores conectados a ele que são chamados clientes. Cada cliente (computador que compõe este tipo de rede) que deseja conectar-se a um determinado serviço ou recurso faz essa solicitação ao servidor da rede, por isso o nome cliente-servidor.

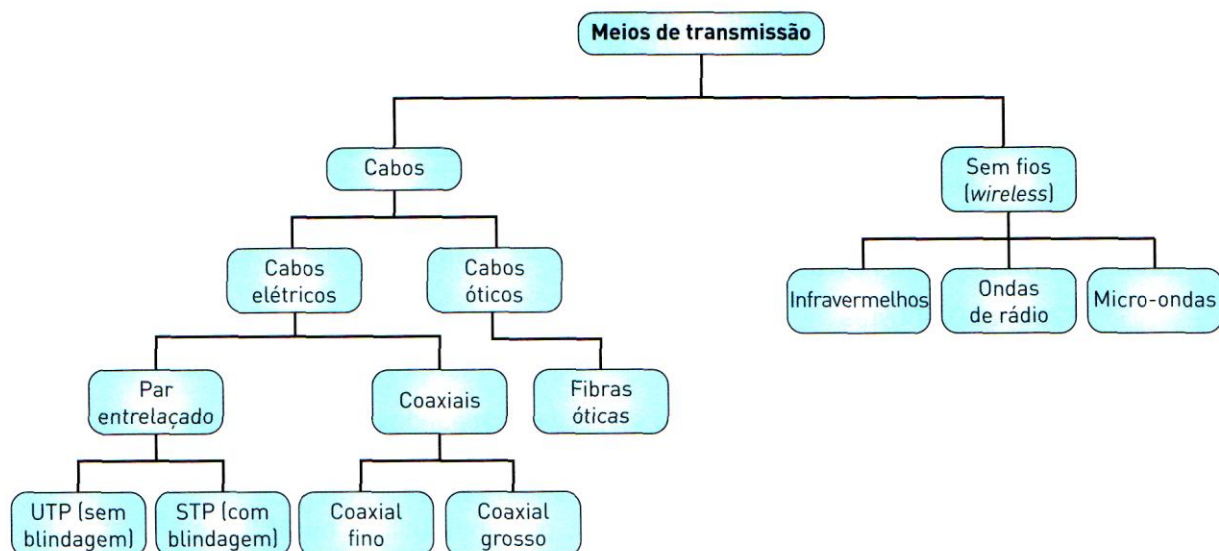
Esse tipo de rede surgiu da necessidade de criar uma estrutura que centralizasse o processamento em um computador central da rede (no caso o servidor, com recursos de *hardware* preparados para tal processamento). Como exemplos de serviços de rede que um servidor pode executar estão: servidor de aplicativos, serviço de impressão, hospedagem de *sites*, servidor de *e-mail*, servidor de ficheiros, entre outros.

Os computadores clientes, também chamados de “nós” em uma rede de computadores, são as estações de trabalho ou *desktops*. Os computadores clientes são utilizados pelos utilizadores que acedem a às informações armazenadas no servidor e executam aplicações locais. Como características deste tipo de rede podemos citar:

- Maior custo e implementação mais complexa que uma rede do tipo ponto-a-ponto.
- Existência de pelo menos um servidor da rede.
- Redes do tipo cliente-servidor, apresentam uma estrutura de segurança melhorada, pois as informações encontram-se centralizadas no servidor, o que facilita o controle e o gerenciamento dos mesmos.
- Neste tipo de rede não há tolerância a falhas (como existe em um sistema descentralizado) haja vista um único sistema centralizado de informações (servidor).
- Um servidor de rede é um computador projetado (*hardware*) para suportar a execução de várias tarefas que exigem bastante do *hardware* (como disco rígido e processador), diferentemente de uma estação de trabalho (cliente), que não possui características para realizar o trabalho de um servidor (quando falamos puramente do *hardware* necessário a um computador servidor).
- No contexto do *software* para servidores, deve prover serviços usuais para atender os clientes da rede: autenticação, compartilhamento de recursos, entre outros.

MEIOS FÍSICOS DE TRANSMISSÃO

Para que seja possível a transmissão de dados numa rede, tem de existir algum meio físico de transmissão de sinal. Dentro dos diversos meios de transmissão de sinais existentes, podemos considerar a utilização de cabos de cobre, cabos de fibra ótica, ou uma transmissão sem fios (*wireless*).



CABOS ELÉTRICOS

CABOS DE PAR TRANÇADO - CATEGORIAS, BLINDAGEM, APLICAÇÕES

Cabos de par trançado são usados para transmitir sinais em sistemas de telecomunicação e redes de computadores. Os cabos de par trançado mais populares são compostos por quatro pares de fios de cobre isolados trançados. A torção reduz fortemente a influência da interferência eletromagnética externa e a interferência mútua entre os pares, chamada crosstalk. Atualmente, os cabos são usados principalmente em redes de telefones e Ethernet.

Este artigo apresenta os tipos de cabos de par trançado e sua classificação baseada na categoria, estrutura, aplicação, parâmetros de transmissão.

Categorias/classes de cabos de par trançado

Categorias/classes de cabos de par trançado permitem que os usuários selecionem cabos adequados para aplicações em diferentes redes e garantam compatibilidade retroativa com as soluções existentes. Os requisitos para categorias específicas ou classes de cablagem estruturada (incluindo questões de compatibilidade) são definidos pela Telecommunications Industry Association (TIA) e pela International Organization for Standardization (ISO). O padrão EIA/TIA e o padrão europeu EN50173 definem vários grupos de cabos de cobre com diferentes capacidades de transmissão de dados.

- Categoria 1 (classe A pela EN 50173)

Serviços de voz por telefone com banda até 100 kHz.

- Categoria 2 (classe B pela EN 50173)

Serviços de voz e sistemas de terminais mais antigos com banda até 1 MHz.

- Categoria 3 (classe C pela EN 50173)

Serviços telefónicos com banda até 16 MHz.

- Categoria 5/5e (classe D pela EN 50173))

A categoria de cabo de par trançado de computador usado com mais frequência em redes locais, incluindo aplicativos que requerem banda de frequência de até 100 MHz (FastEthernet 100Base-TX, GigabitEthernet 1000Base-T).



Cabo CAT 5e UTP para aplicações interiores
NETSET U/UTP 5e [E1408](#)



Cabo CAT 5e UTP para aplicações exteriores
NETSET U/UTP 5e (gel-filled, preto) [E1410](#)



Cabo Cat 5e UTP NETSET U/UTP (PE - exterior) [E1412](#)



Cabo Blindado CAT 5e NETSET F/UTP 5e (interior) [E1515](#)



Cabo Blindado at5e NETSET BOX F/UTP 5e (exterior) [E1517](#)

- Categoria 6 (classe E by EN 50173)

Aplicações que requerem faixa de frequência de até 250 MHz, taxas de transferência de dados de até 1 Gbps.



Cabo CAT 6 NETSET U/UTP 6 (interior) [E1608](#)

- Categoria 6A (classe E_A da EN 50173)

Aplicativos que requerem faixa de frequência de até 500 MHz. Ideal para transmissões multimídia; U/FTP, versões F/FTP.



Cabo blindado CAT 6A U/FTP NETSET U/FTP 6A (interno) [E1616](#) [500](#)

- Categoria 7 (classe F por EN 50173)

Os cabos da categoria 7 permitem aplicações que requerem faixa de frequência de até 600 MHz. Em comparação com as categorias mais baixas, cada par dos cabos S/FTP é exibido individualmente e todos os pares são envolvidos em outra camada de proteção. Os conectores para os cabos também são blindados.

- Categoria 7A (classe F_A da EN 50173)

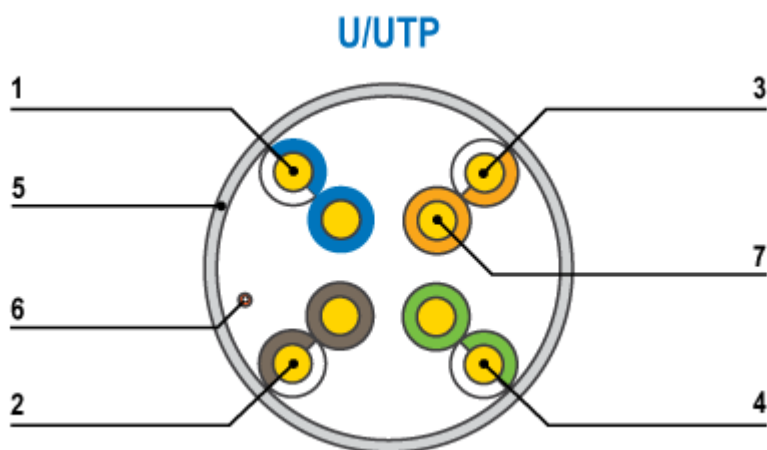
Aplicações que requerem banda de frequência até 1000 MHz. Permite taxas de transferência de dados de até 100 Gbps em distâncias de até 15 m ou 40 Gbps em distâncias de até 100 m.

Blindagem

O uso de blindagem elétrica garante que os sinais transmitidos pelos pares sejam menos suscetíveis à interferência ambiental e, analogicamente, criam níveis mais baixos de interferência eletromagnética externa. No entanto, o uso de cabos blindados requer conhecimento dos princípios de blindagem adequada e sua implementação prática, incluindo conexões equipotenciais e infraestrutura de aterramento no (s) edifício(s). O princípio básico é aterrar adequadamente a tela nas duas extremidades dos cabos.

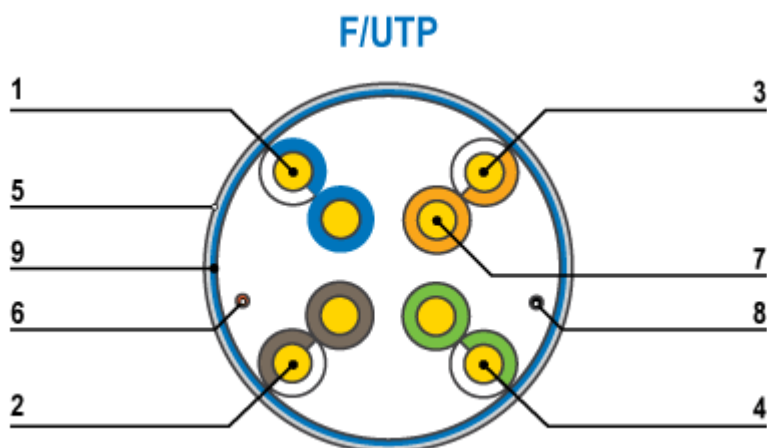
Tipos de cabos de par trançado:

- U/UTP – sem blindagem



1. Par de fios branco-azul/azul
2. par de fios branco-marrom/marrom
3. Par de fios branco-laranja/laranja
4. par de fios branco-verde/verde
5. Jaqueta/bainha
6. Cabo Rip-cord
7. Condutor central (aplica-se a todos os fios)

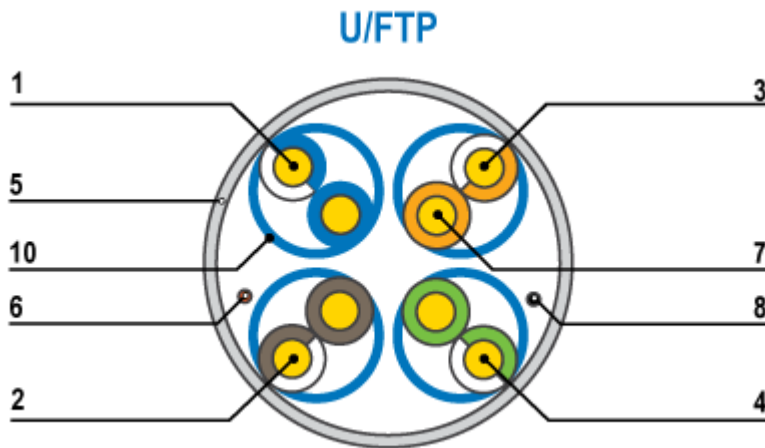
- F/UTP – cabo blindado de alumínio com pares trançados não blindados



1. Par de fios branco-azul/azul
2. par de fios branco-marrom/marrom
3. Par de fios branco-laranja/laranja
4. par de fios branco-verde/verde

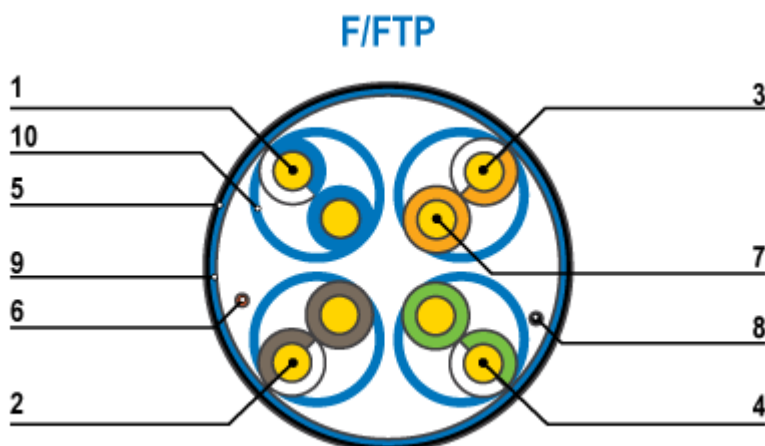
5. Jaqueta/bainha
6. Cabo Rip-cord
7. Conductor central (aplica-se a todos os fios)
8. Fio de drenagem
9. Blindagem do cabo

- U/FTP – cabo com pares trançados individualmente blindados



1. Par de fios branco-azul/azul
2. par de fios branco-marrom/marrom
3. Par de fios branco-laranja/laranja
4. par de fios branco-verde/verde
5. Jaqueta/bainha
6. Cabo Rip-cord
7. Conductor central (aplica-se a todos os fios)
8. Fio de drenagem
9. Emparelhar escudo (aplica-se a todos os pares)

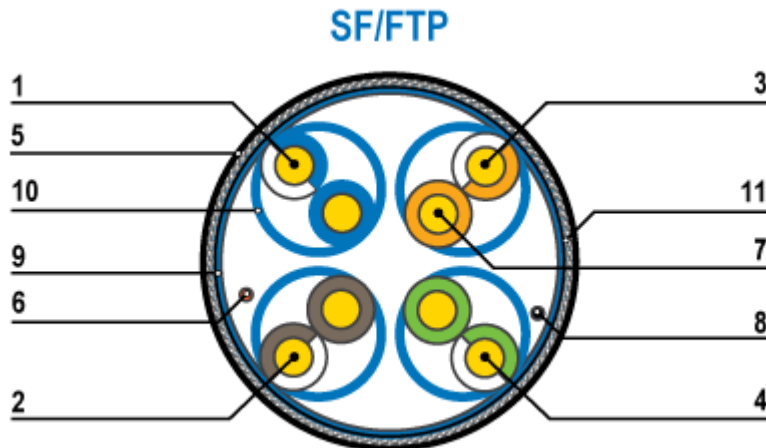
- F/FTP – cabo blindado de folha com pares trançados individualmente blindados



1. Par de fios branco-azul/azul
2. par de fios branco-marrom/marrom
3. Par de fios branco-laranja/laranja
4. par de fios branco-verde/verde
5. Jaqueta/bainha

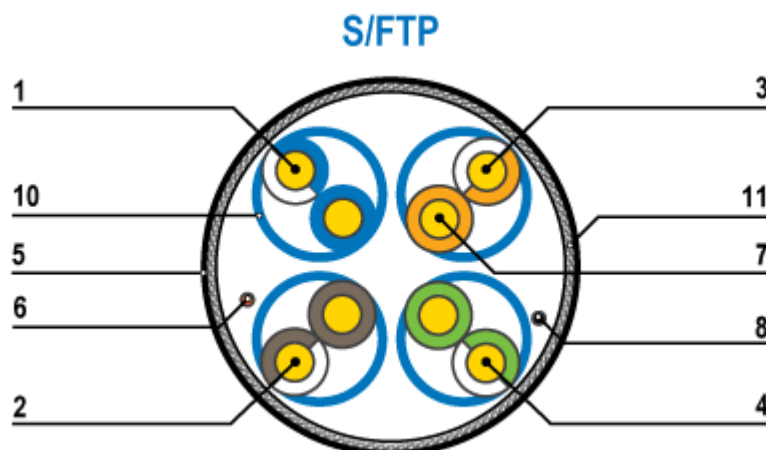
6. Cabo Rip-cord
7. Condutor central (aplica-se a todos os fios)
8. Fio de drenagem
9. Blindagem do cabo
10. Emparelhar escudo (aplica-se a todos os pares)

- SF/FTP – cabo blindado de trança e folha com pares trançados individualmente protegidos por folha



1. Par de fios branco-azul/azul
2. par de fios branco-marrom/marrom
3. Par de fios branco-laranja/laranja
4. par de fios branco-verde/verde
5. Jaqueta/bainha
6. Cabo Rip-cord
7. Condutor central (aplica-se a todos os fios)
8. Fio de drenagem
9. Blindagem do cabo da folha
10. Emparelhar escudo (aplica-se a todos os pares)
11. Braid screen

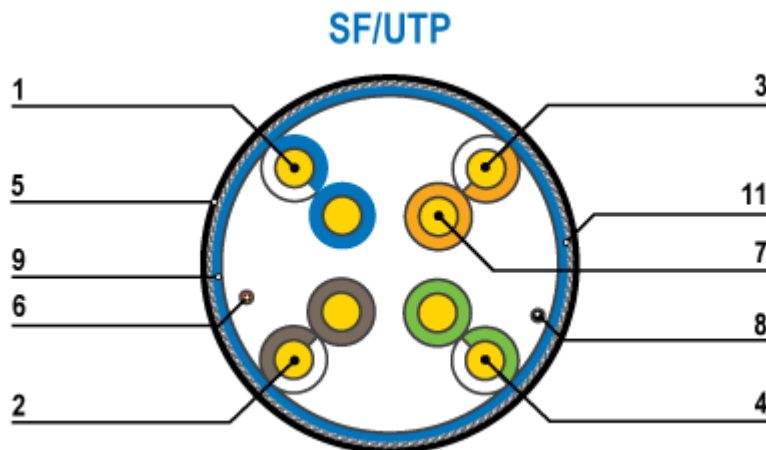
- S/FTP – cabo blindado de trança e folha com pares trançados individualmente protegidos por folha



1. Par de fios branco-azul/azul
2. par de fios branco-marrom/marrom

- 3. Par de fios branco-laranja/laranja
- 4. par de fios branco-verde/verde
- 5. Jaqueta/bainha
- 6. Cabo Rip-cord
- 7. Condutor central (aplica-se a todos os fios)
- 8. Fio de drenagem
- 10. Emparelhar escudo (aplica-se a todos os pares)
- 11. Braid screen

- SF/UTP – cabo blindado de trança e folha com pares trançados não blindados



- 1. Par de fios branco-azul/azul
- 2. par de fios branco-marrom/marrom
- 3. Par de fios branco-laranja/laranja
- 4. par de fios branco-verde/verde
- 5. Jaqueta/bainha
- 6. Cabo Rip-cord
- 7. Condutor central (aplica-se a todos os fios)
- 8. Fio de drenagem
- 9. Blindagem do cabo da folha
- 11. Braid screen

Aplicações

Existem dois grupos distintos de cabos, para aplicações externas e internas.

- Exterior

A característica mais importante dos cabos externos é sua resistência a condições ambientais difíceis e mutáveis. A principal influência desta característica é o tipo e a qualidade do material usado na capa. Existem cabos disponíveis com revestimento de PVC e polietileno (PE). O PE é mais duro do que o PVC, possui maior resistência mecânica e resistência química, e faz uma barreira melhor contra gases.

- Interior

Ao usar cabos dentro de edifícios, deve ser dada uma atenção especial aos requisitos relativos à reação da fiação ao fogo. Os tipos dedicados de isolamento, por exemplo polímeros LSOH ou LSZH (Low Smoke Zero Halogen), são seguros quando expostos ao fogo. Em comparação com o PVC, o PE não produz substâncias nocivas e tóxicas (halogênios), e também não gera grandes quantidades de fumaça. O uso de cabos em revestimentos LSZH é muitas vezes uma exigência dos regulamentos de incêndio em grandes edifícios.

Taxas de transferência de dados

A câmara DS-2CD2043G0-I é dedicada para sistemas profissionais de CFTV IP. A câmara compacta foi equipada com sensor CMOS de 4 MP e 1/3" de alta qualidade, proporcionando boa cobertura de vídeo, mesmo em condições de pouca luz. Juntamente com o iluminador IR com alcance de até 30 m, a câmara também pode operar em escuridão total. -Em lente de 2,8 mm tem ângulo de visualização de 98. A carcaça com classificação IP67 da câmara protege os componentes eletrônicos contra condições climáticas adversas. A câmara pode ser alimentada convencionalmente com uma fonte de 12 VDC ou com o uso da opção PoE (802.3af).

- Categoria 3 (classe C da EN 50173)
 - o 4 Mb/s - (10BaseT, RS 232)
- Categoria 5 (classe D da EN 50173)
 - o 1 Gb/s - (1000BaseT, ATM 155)
- Categoria 6 (classe E da EN 50173)
 - o 1 Gb/s - (1000BaseT)
 - o 10 Gb/s - (10GBASE-T até 55m)
- Categoria 6A (classe E_A da EN 50173)
 - o 10 Gb/s - (10GBASE-T)

Desempenho de fogo dos cabos

Até agora, os condutores e cabos eram tratados exclusivamente como produtos elétricos sujeitos a regulamentos de segurança do produto sob a Diretriz de Baixa Tensão (LVD) e estavam sujeitos à marcação CE pelo fabricante. As novas regras estabelecidas pela EN50575 impõem aos fabricantes (também importadores e distribuidores) a obrigação de comissionar testes relevantes a organismos / laboratórios de certificação notificados para obter certificados confirmando as classes de resistência ao fogo de seus produtos e emitir Declarações de Desempenho (DoP). com os Euroclasses relevantes. O Euroclasse de um produto de construção (incluindo cabos de alimentação, controlo e comunicação) permite a sua classificação em termos de reação ao fogo de acordo com as mesmas regras e critérios em toda a Europa. As marcações da classificação de incêndio já podem ser encontradas nos rótulos de muitos produtos de construção e em breve serão necessárias para todos esses produtos.

| Euroclass | Test methods | Additional classification | Examples of products |
|------------------|--------------------------|---|----------------------------------|
| A _{ca} | EN ISO 1716 | - | halogen-free cables |
| B1 _{ca} | EN 50399 EN 60332-1-2 | smoke production (s1, s2), flaming droplets/particles (d1,d2) and acidity (a1) | halogen-free cables |
| B2 _{ca} | EN 50399 EN 60332-1-2 | | hard PVC and halogen-free cables |
| C _{ca} | EN 50399 EN 60332-1-2 | | halogen-free cables |
| D _{ca} | EN 50399 EN 60332-1-2 | | high-quality PVC cables |
| E _{ca} | EN 60332-1-2 | no performance determined | PVC cables |

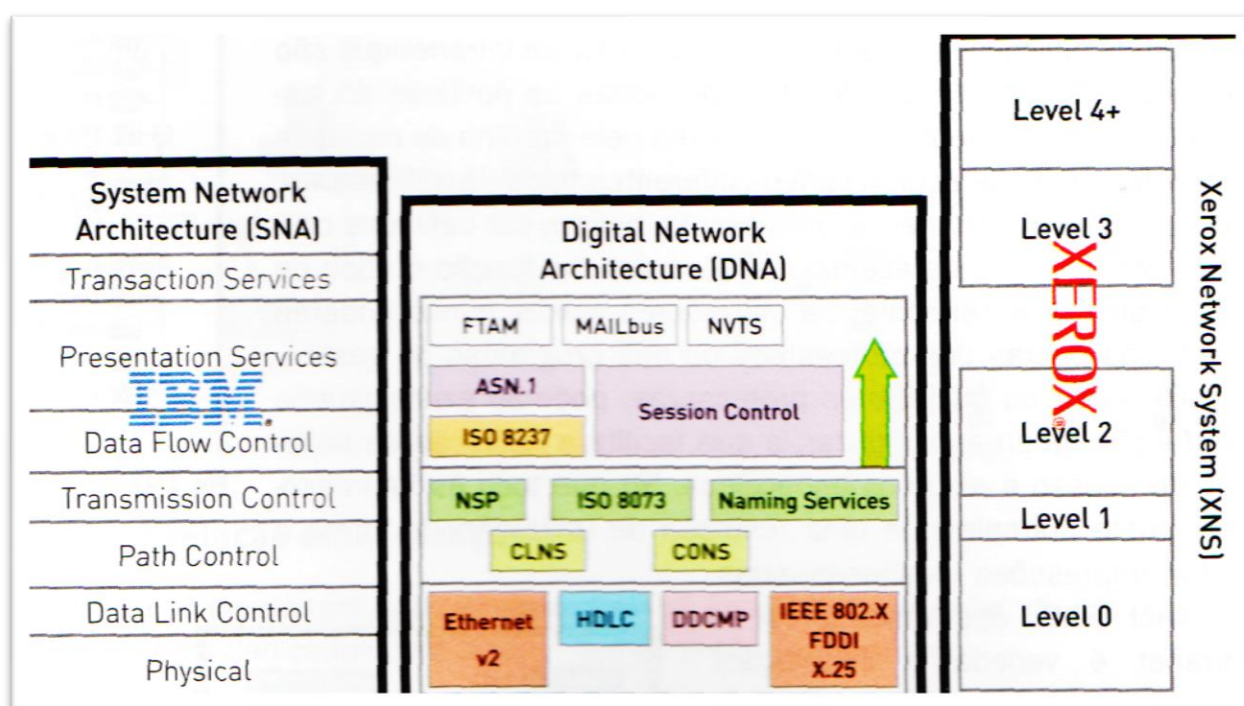
| | | | |
|-----------------|---|---------------------------------|-------------------|
| | | (NPD) | |
| F _{ca} | Not fulfilling requirements for E _{ca} | no performance determined (NPD) | PE and PVC cables |

Esquema de classificação de cabos de acordo com a norma EN50575

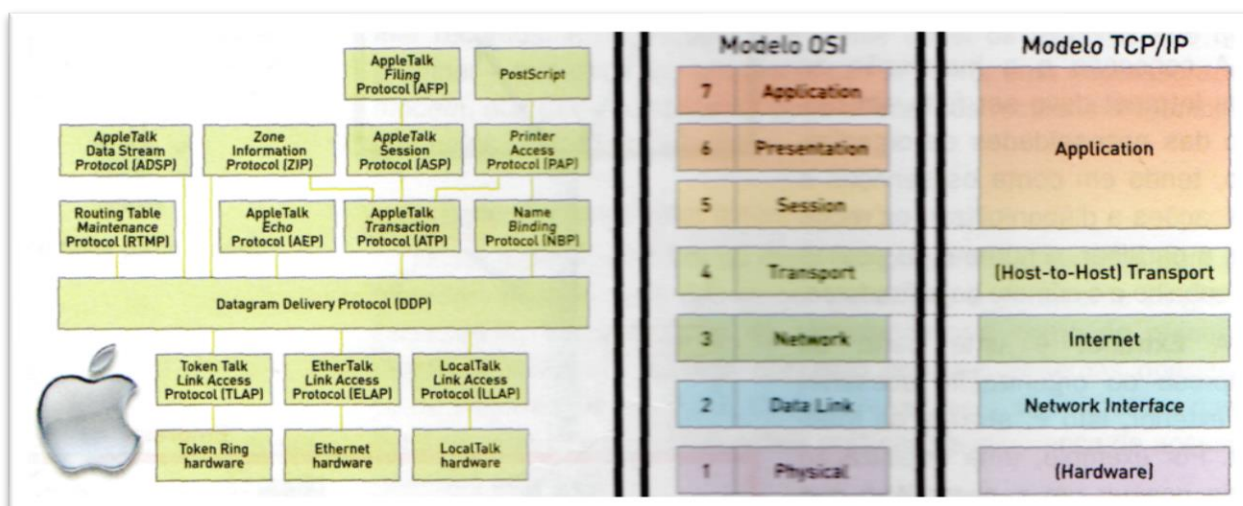
A IMPORTÂNCIA DAS ATIVIDADES DE NORMALIZAÇÃO

NOÇÃO DE NORMA E DE NORMALIZAÇÃO

Nos anos 80. as empresas de telecomunicações criavam as suas próprias infraestruturas de rede. Assim, empresas como a IBM, AT&T, DEC, etc., possuíam sistemas proprietários: os sistemas instalados eram diferentes de empresa para empresa.



Arquiteturas de rede - I



<https://www.embarcados.com.br/redes-de-comunicacao-em-rs-485/>

Esta situação obrigava os clientes a dependerem apenas de uma empresa e dificultava muito a expansão da rede e a integração de novos equipamentos e o acesso/disponibilização de novos serviços.

Assim, existiam cablagens não estruturadas de todos os tipos: eletricidade, segurança, controlo, voz, dados, etc.

No início da década de 90, a associação EIA/TIA (*Electronic Industries Association / Telecommunications Industry Association*) publicou a primeira versão de uma norma de padronização de fios e cabos para telecomunicações em prédios, denominada de EIA/TIA-568 com o seguinte objetivo:

- ⇒ "obrigar" os diferentes fornecedores a respeitar um padrão genérico de cablagem de telecomunicações;
- ⇒ estruturar um sistema de cablagem dentro de um edifício e entre edifícios, com equipamentos de diferentes fabricantes;
- ⇒ definir critérios técnicos de desempenho para sistemas de cablagens diferentes.

ORGANIZAÇÕES DE NORMALIZAÇÃO: ISO, ISOC, IEC, IEEE

Como foi referido, os padrões para as redes são definidos por diferentes entidades, normalmente sem fins lucrativos, que privilegiam o consenso dos diferentes fabricantes.

Descrevemos seguidamente as organizações de normalização mais relevantes: *ISO - International Organization for Standardization*

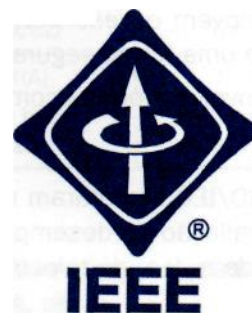
- ⇒ define as normas que devem ser observadas no segmento cablagens;
- ⇒ certifica os novos produtos a colocar no mercado;
- ⇒ criou o modelo OSI.



ISO



Modelo OSI



IEEE

ISOC - Internet Society

Define as normas da Internet tendo por objetivo a sua melhoria e expansão. Um dos seus grandes objetivos é integrar o maior número possível de tecnologias inovadoras.



Internet Society

IEC - International Electrotechnical Commission



- ↪ publica padrões para tecnologias eletrónicas e apoia a segurança, o desempenho, a satisfação e o ambiente. Certifica os componentes antes de serem lançados no mercado.

Assim, o processo de normalização/padronização tem possibilitado muitas vantagens, nomeadamente:

- ↪ a criação e expansão de infraestruturas de redes e comunicação;
- ↪ a gestão da rede;
- ↪ a integração de diferentes equipamentos numa rede;
- ↪ a comunicação entre dispositivos diferentes;
- ↪ a transferência segura e eficaz de dados;
- ↪ as normas da ISO e da IEC garantem que, respetivamente, todas as normas informáticas ou eletrónicas integradas nos equipamentos novos sejam aprovadas para depois serem vendidas ao público;
- ↪ garantem a qualidade dos produtos e a maior performance possível;
- ↪ normas como a ISOC promovem o desenvolvimento da Internet e de novas tecnologias e aplicações de uma forma segura e útil para todos;
- ↪ a IEEE tem procurado desenvolver normas com velocidades cada vez maiores, principalmente nas redes.

As organizações EIA/TIA e ISO/IEC elaboraram normas e procedimentos, sob o ponto de vista da instalação, avaliação de desempenho e soluções de problemas, para a integração da cablagem de redes, de telecomunicações e de controlo, para forçar/garantir os serviços.

PADRÕES E ARQUITETURAS DE REDES

Quando se começaram a usar redes de computadores, no início dos anos 70, essa iniciativa partiu de diversos fabricantes que desenvolveram tecnologias de forma mais ou menos independente entre si.

| Arquiteturas proprietárias | | |
|----------------------------|------------------------------------|---|
| Fabricante | Arquitetura | Situação atual |
| IBM | SNA - Systems Network Architecture | Utilização decrescente com a adoção do TCP/IP pela IBM. |
| DIGITAL | DNA - Digital Network Architecture | Abandonada. |

| | | |
|-----------------------|-----------------------------|---------------------------|
| XEROX | XNS - Xerox Network Systems | Abandonada. |
| Apple | AppleTalk | Utilização decrescente. |
| Novell | Novell Netware | Mantém alguma utilização. |
| Microsoft/3Com/HP/IBM | Lan Manager | Abandonado. |
| Banyan Systems | VINES | Abandonado. |
| IBM (Sytek) | NetBIOS | Utilização generalizada. |

Arquiteturas proprietárias - <https://www.dei.isep.ipp.pt/~asc/doc/arquitecturas.html>

Todas estas tecnologias proprietárias foram, inicialmente, mantidas em grande segredo, o que impossibilitava a sua interligação. Quando uma instituição optava por determinado fabricante, ficava irremediavelmente dependente desse fabricante, sob pena de ter de substituir toda a rede.

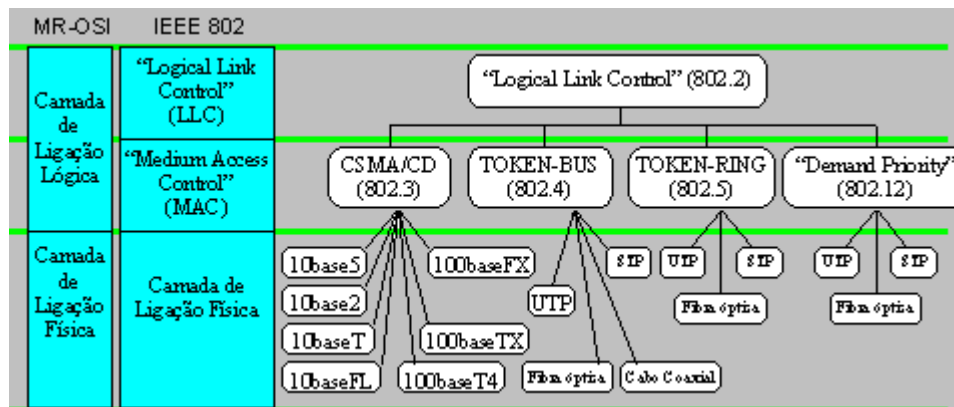
Em resposta a esta situação foram sendo desenvolvidos padrões e modelos de arquiteturas de rede que permitissem a interligação e a integração dos diferentes sistemas existentes. Neste sentido foram desenvolvidos:

- ⇒ o modelo OSI, *Open Systems Interconnection*, pela ISO (*International Organization for Standardization*), nos anos 70 e 80 do século XX, que estabeleceu um conjunto de normas que os fabricantes deveriam seguir de forma a permitir a sua interligação; os sistemas que seguem estas normas passariam a ser considerados "sistemas abertos";
- ⇒ o padrão IEEE 802, que definiu *standards* para as redes (tabela seguinte).

| Nível | N.º Norma | | |
|------------------|---|---|--|
| LIGAÇÃO DE DADOS | IEEE 802.2 (LLC) | | |
| | IEEE 802.3 Acesso a meios CSMA/CD | IEEE 802.4 Acesso a meios TOKEN BUS | IEEE 802.5 Acesso a meios TOKEN RING |
| FÍSICO | COAXIAL Banda base 50 Ω | COAXIAL Banda larga 75 Ω | PAR ENTRANÇADO |

Norma IEEE 802

Atualmente, existem outros standards, nomeadamente, standards para redes de fibra ótica, redes metropolitanas, etc. Entre implementações LAN e WAN, a diversidade é enorme, a título de exemplo apresenta-se o caso da arquitetura [IEEE 802](#) muito generalizado nas LAN e com várias camadas bem definidas:



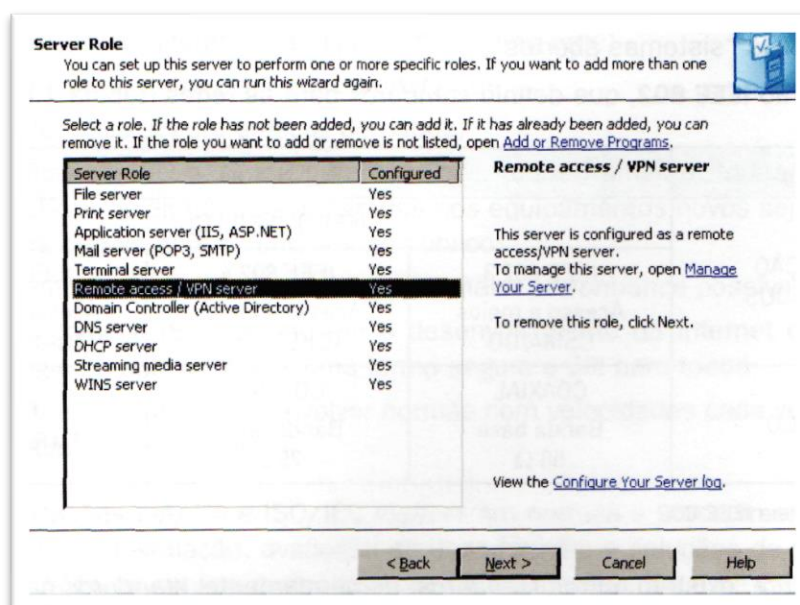
Como se pode observar a camada 2 do modelo OSI aparece aqui dividida em duas subcamadas, LLC e MAC, embora não ilustrado na figura, também a camada 1 pode ser dividida em duas subcamadas PLS/PMI e MDI.

AS TAREFAS DOS COMPUTADORES NA REDE

Um servidor de rede é um computador que disponibiliza vários recursos partilhados aos clientes e a outros servidores que possam existir na rede. Os recursos partilhados podem incluir espaço em disco, acesso às impressoras, scanners, acesso à Internet, *e-mail*, etc. Qualquer computador pode funcionar como servidor de rede. O que diferencia um servidor de uma estação de trabalho (workstation) não é o *hardware*, mas sim a sua função na rede. Em termos gerais, uma estação de trabalho é um computador utilizado por um indivíduo para executar as suas tarefas, enquanto um servidor é uma máquina onde são executadas as políticas do sistema. Existem muitas instalações onde o servidor funciona também como estação de trabalho, mas este é um exemplo de uma prática não recomendada.

Os servidores são habitualmente máquinas muito mais robustas do que as estações de trabalho, quer em termos de capacidade de processamento, espaço de armazenamento quer de memória RAM e têm instalados sistemas operativos para servidores. Desta forma, o custo destes servidores é muito elevado. Contudo, o facto de poder executar tarefas de gestão da rede de forma centralizada permite uma boa amortização dos custos globais para a organização. Não havendo um servidor, as tarefas de gestão da rede teriam de ser executadas num ou em vários postos de trabalho, dificultando a administração do sistema e podendo criar graves problemas de segurança.

Numa organização de média dimensão, um único servidor pode ser configurado para executar várias funções na rede como, por exemplo, servidor de ficheiros, servidor de impressão, servidor de DHCP e DNS, ou ainda servidor de *e-mail*, servidor de fax, servidor de autenticação, etc.



Funções do servidor

Vejamos alguns destes tipos de servidor

SERVIDORES DE FICHEIROS E IMPRESSORAS

Em qualquer organização existem impressoras partilhadas que permitem aos utilizadores a impressão de documentos. Algumas impressoras são de grande qualidade e funcionam também como scanners e

fotocopiadoras. Nos últimos tempos tem-se abandonado a utilização de uma impressora para cada posto de trabalho. Assim, as empresas diminuem substancialmente os custos na aquisição de consumíveis e na manutenção, optando por adquirir equipamentos mais robustos que servem um maior número de utilizadores. Estas impressoras são ligadas a uma porta de rede sendo o serviço de impressão executado no servidor ou num posto de trabalho configurado para o efeito. Outras impressoras de menores dimensões são simplesmente ligadas à porta USB de um posto de trabalho e depois partilhada.

Da mesma forma, o software e os documentos também são disponibilizados a partir de uma localização centralizada, o servidor de ficheiros, podendo ser acedidos de acordo com as políticas de partilha definidas pelo administrador da rede.

Os servidores de ficheiros permitem não só a disponibilização de ficheiros, mas também uma gestão centralizada das quotas de disco dos utilizadores. Esta gestão centralizada facilita obviamente a criação de cópias de segurança.

SERVIDORES DE DHCP

De forma a reduzir os esforços de configuração manual dos endereços IP dos computadores da Intranet é muitas vezes configurado o servidor de DHCP.

Um servidor de DHCP atribui endereços IP aos computadores clientes. Todos os endereços IP de todos os computadores são armazenados numa base de dados que reside numa máquina servidor. Em muitas instalações são criadas reservas de IP de forma a garantir que determinados dispositivos (computadores, impressoras, routers, etc.) tenham sempre o mesmo IP.

SERVIDORES DE DNS

Um servidor de DNS é um computador que traduz os nomes na rede em endereços IP. Por exemplo, se num dos computadores da rede for digitado o endereço `www.portoeditora.pt`, o servidor de DNS traduz este nome amigável para o IP correspondente (neste caso, `195.23.51.110`). Esta tradução de nomes para IP é efetuada também quando se tenta localizar um computador na Intranet, como, por exemplo, `(\\nome_do_posto)`.

SERVIDORES DE EMAIL

Os servidores de email são computadores da rede que funcionam como uma estação de correios virtual; consiste numa área de armazenamento onde são guardados os e-mails dos utilizadores. Os e-mails são enviados do servidor para g os postos de trabalho de acordo com as informações de encaminhamento definidas pelo utilizador.

SERVIDORES DE BASE DE DADOS

Os servidores de base de dados armazenam grandes quantidades de informação num local centralizado. Frequentemente, esta informação é replicada noutros l servidores de forma a diminuir os tempos de acesso. Por exemplo, ao consultar os f rendimentos anuais de um contribuinte, na base de dados nas finanças, é enviada | para o computador do utilizador apenas a informação solicitada.

SERVIDORES DE FAX

O servidor de fax (ou fax server) é um pequeno sistema instalado numa LAN que permite aos postos enviar e

receber mensagens de fax. As mensagens de fax são armazenadas como documentos de texto ou imagens. Os documentos digitalizados podem ser enviados como mensagens de fax.

O fax server é um computador onde se encontra instalado um programa de fax, o fax-modem, com uma ligação à linha telefónica ou à Internet e está disponível aos utilizadores da rede.

PRINCIPAIS DISPOSITIVOS DE UMA REDE

Uma rede de computadores é composta por diferentes dispositivos, cada um com sua função, com o objetivo de dar funcionalidade e organização, bem como, prover a comunicação entre os diferentes componentes de uma rede.

A seguir são citados os principais dispositivos de uma rede de computadores, com o intuito de conhecermos um pouco melhor os principais componentes que compõem uma rede:

- ⇒ **Host** – equipamento utilizado pelos usuários finais para processamento das aplicações e conexão à rede. Enquadram-se nesta descrição os *portáteis*, tablets, computadores pessoais, entre outros.
- ⇒ **Interface de rede** – cada computador, entre outros dispositivos conectam-se a uma rede de computadores através de uma placa de rede. A esta placa de rede é dado o nome de interface de rede. Uma placa de rede pode ser do tipo Ethernet cabeada (na qual um cabo é conectado a esta placa) ou então Ethernet sem-fios (placas que se comunicam via Bluetooth, ondas de rádio, etc.). Características como velocidade, modo de funcionamento e barramento de conexão, podem variar de uma interface para outra.
- ⇒ **Hub** – o *hub* (concentrador) é um dispositivo cuja função é interligar os computadores de uma rede local. O funcionamento do *hub* se difere de um *switch*, pois o *hub* simplesmente repassa o sinal vindo de um computador para todos os computadores ligados a ele (como um barramento).
- ⇒ **Switch** – semelhante ao *hub*, um *switch* serve de concentrador/ comutador numa rede de computadores com a diferença de que recebe um sinal vindo de um computador origem e entrega este sinal somente ao computador destino. Isto é possível devido à capacidade destes equipamentos em criar um canal de comunicação exclusivo (origem/destino). Esta prática diminui consideravelmente o número de **colisões**¹ e a perda de **pacotes**² na rede.
- ⇒ **Bridge** – ponte de ligação entre duas ou mais redes. Como exemplo, podemos citar uma ponte entre uma rede cabeada e uma rede sem-fio.
- ⇒ **Gateway** – sinonimo de router na arquitetura TCP/IP, é o equipamento que conecta os *hosts* à rede. Em outras arquiteturas de redes, um *gateway* é um dispositivo (*hardware* ou *software*) que converte mensagens de um protocolo em mensagens de outro protocolo.

¹ **Colisões** - São perdas de pacotes ocasionadas quando dois ou mais hosts tentam transmitir dados simultaneamente utilizando o mesmo meio físico.

² **Pacote** - É a forma como é chamado um conjunto de dados enviado através da rede.

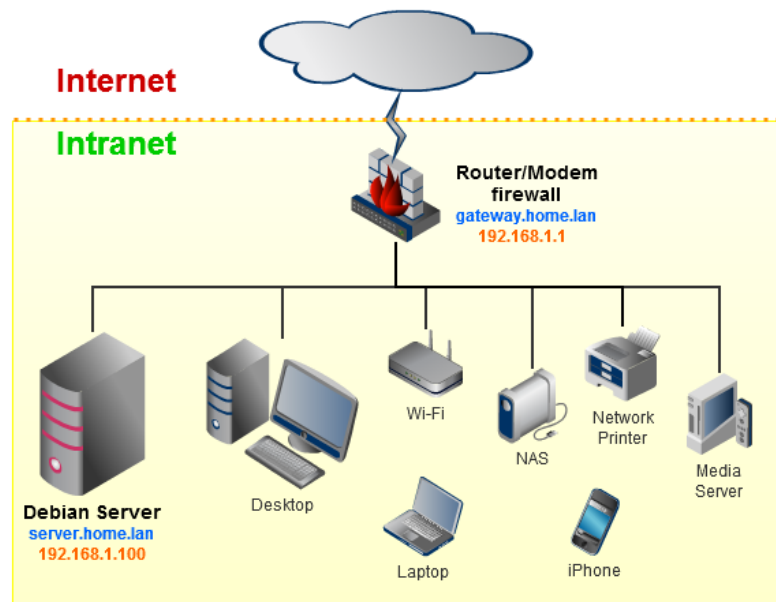
INTRANET E EXTRANET

A **Intranet** é uma rede informática de uma empresa ou organização construída com base nos protocolos da Internet. Uma Intranet é normalmente uma rede do tipo cliente-servidor onde os utilizadores possuem credenciais, isto é, nome de utilizador e palavra-passe, que lhes permitem aceder aos recursos e à informação disponibilizada.

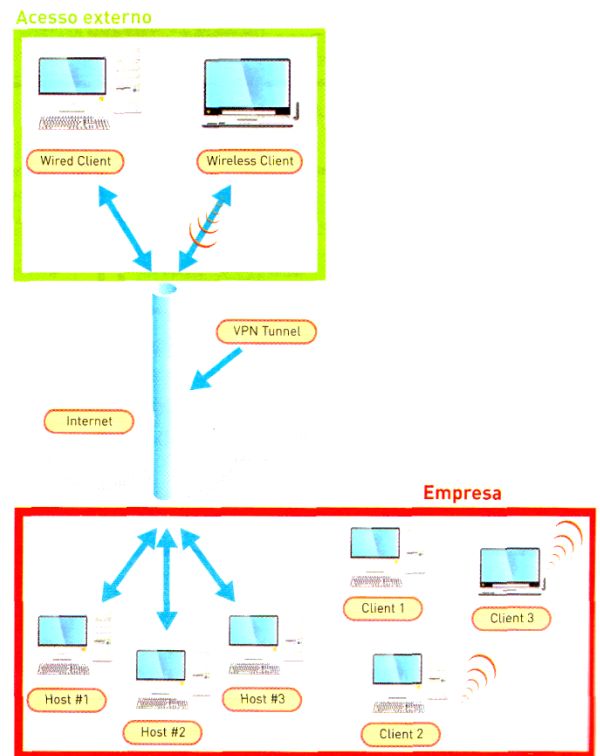
Mesmo em pequenas organizações, existe um servidor na Intranet onde se encontra instalado um sistema

operativo servidor e algumas aplicações de gestão. É no servidor da Intranet que são definidas, pelo administrador da rede, todas as políticas do sistema. A definição destas políticas passa pela partilha de recursos e de informação de acordo com os diferentes tipos de utilizadores. Por exemplo, na Intranet de uma escola, podem ser definidas políticas diferenciadas de acesso aos recursos em função do tipo de utilizadores. Naturalmente, os utilizadores alunos nunca poderão aceder às pastas dos professores ou aos programas de gestão. Mesmo entre os utilizadores professores, poderão existir grupos em função da área disciplinar, o que facilita a definição de políticas de acesso a recursos específicos. No que toca às impressoras, existe normalmente uma restrição de utilização de forma a evitar impressões desnecessárias. À maior parte dos utilizadores da Intranet é vedada a instalação/ desinstalação de software. Existem um ou dois acessos à Internet e o acesso aos recursos do setor administrativo é igualmente restrito.

A conceção e a instalação de uma **Intranet** deve ser feita em função das necessidades da organização, tendo em conta os serviços e aplicações a disponibilizar, os recursos a partilhar, o número de postos de trabalho e o número de utilizadores.



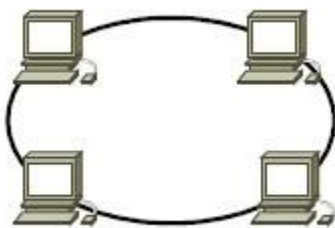
A **Extranet** é uma parte da empresa ou organização acessível do exterior, isto é, através da Internet. Por exemplo, uma organização pode possuir um servidor *Web* que disponibiliza uma página *Web* na Internet. Como não podia deixar de ser, podem existir, nessa página, zonas de acesso geral e outras de acesso reservado. A parte restrita pode ser acessível apenas aos utilizadores registados ou aos colaboradores da empresa.



TOPOLOGIAS

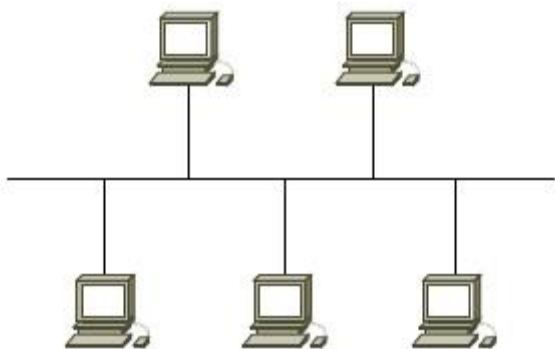
ANEL (*RING*)

Topologia em Anel



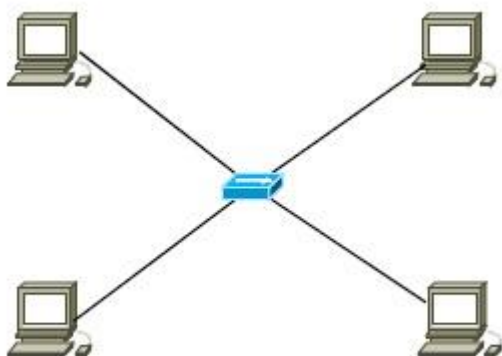
BARRAMENTO (*BUS*)

Topologia em Barramento



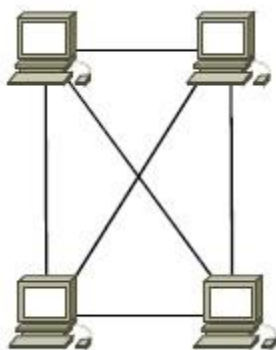
ESTRELA (*STAR*)

Topologia em Estrela

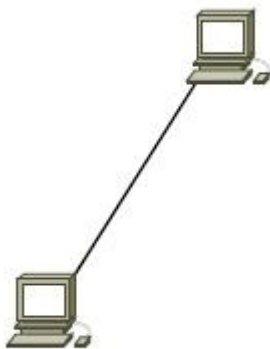


MALHA (*MESH*)

Topologia em Malha

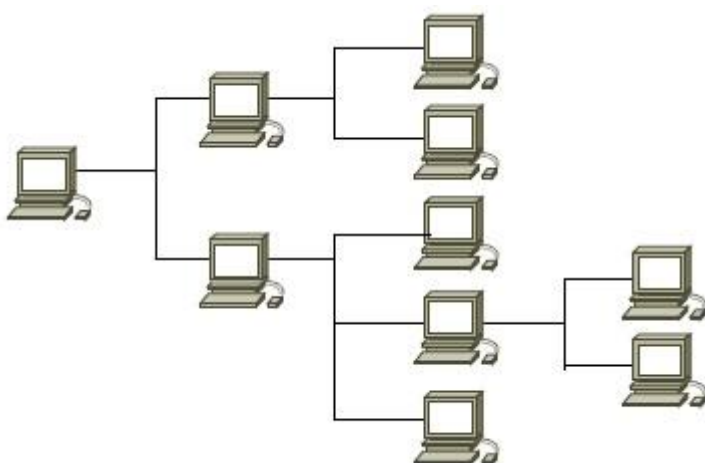


PONTO-A-PONTO (*POINT-TO-POINT*)



ÁRVORE (*TREE*)

Topologia em Árvore



MODELOS DE REFERÊNCIA OSI

O modelo OSI (*Open Systems Interconnection*) foi desenvolvido pela ISO (*International Standard Organization*) com o objetivo de criar uma estrutura para definição de padrões para a conectividade e interoperabilidade de sistemas heterogêneos.

Define um conjunto de 7 camadas (*layers*) e os serviços atribuídos a cada uma.

O modelo OSI é uma referência e não uma implementação.

O objetivo de cada camada é:

- Fornecer serviços para a camada imediatamente superior.
- Esconder da camada superior os detalhes de implementação dos seus serviços.
- Estabelecer a comunicação somente com as camadas adjacentes de um sistema.

Modelo OSI

| | | |
|---------|---|--------------|
| Camadas | 7 | Aplicação |
| | 6 | Apresentação |
| | 5 | Sessão |
| | 4 | Transporte |
| | 3 | Rede |
| | 2 | Enlace |
| | 1 | Física |

DESCRIÇÃO FUNCIONAL DAS CAMADAS

CAMADA 1 – FÍSICA

Transmissão transparente de sequências de bits pelo meio físico.

Contém padrões mecânicos, funcionais, elétricos e procedimentos para acesso a esse meio físico.

Especifica os meios de transmissão (satélite, coaxial, radiotransmissão, par metálico, fibra ótica, etc.).

Tipos de conexão:

- Ponto-a-ponto ou multiponto
- *Full ou half duplex*
- *Serial* ou paralela

CAMADA 2 – ENLACE

Esconde características físicas do meio de transmissão.

Transforma os bits em quadros (*frames*).

Provê meio de transmissão confiável entre dois sistemas adjacentes.

Funções mais comuns:

- Delimitação de quadro
- Detecção de erros
- Sequencialização dos dados
- Controle de fluxo de quadros

Para redes locais é dividido em dois subníveis: LLC (*Logical Link Control*) e MAC (*Media Access Control*).

CAMADA 3 – REDE

Providencia um canal de comunicação independente do meio.

Transmite pacotes de dados através da rede.

Os pacotes podem ser independentes (datagramas) ou percorrer uma conexão pré-estabelecida (circuito)

virtual).

Funções características:

- Tradução de endereços lógicos em endereços físicos
- Roteamento
- Não propaga *broadcast* de rede
- Não possuem garantia de entrega dos pacotes

CAMADA 4 – TRANSPORTE

Nesta camada temos o conceito de comunicação fim-a-fim.

Possui mecanismos que fornecem uma comunicação confiável e transparente entre dois computadores, isto é, assegura que todos os pacotes cheguem corretamente ao destino e na ordem correta.

Funções:

- Controle de fluxo de segmentos
- Correção de erros
- Multiplexação

CAMADA 5 – SESSÃO

Possui a função de disponibilizar acessos remotos, estabelecendo serviços de segurança, verificando a identificação do utilizador, sua senha de acesso e suas características (perfis). Atua como uma interface entre os utilizadores e as aplicações de destino.

Pode fornecer sincronização entre as tarefas dos utilizadores.

CAMADA 6 – APRESENTAÇÃO

Responsável pelas transformações adequadas nos dados, antes do seu envio a camada de sessão. Essas transformações podem ser referentes à compressão de textos, criptografia, conversão de padrões de terminais e arquivos para padrões de rede e vice-versa.

Funções:

- Formatação de dados
- Rotinas de compressão
- Compatibilização de aplicações: sintaxe
- Criptografia

CAMADA 7 - APLICAÇÃO

É responsável pela interface com as aplicações dos computadores (*hosts*).

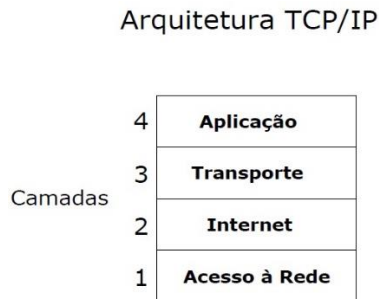
Entre as categorias de processos de aplicação podemos citar:

- Correio eletrónico: X400
- Transferência de arquivos: FTAM
- Serviço de diretório: X500
- Processamento de transações: TP

- Terminal virtual: VT
- Acesso à base de dados: RDA
- Administração de rede

ARQUITETURA TCP/IP

A arquitetura TCP/IP é composta por 4 camadas (formando a pilha da estrutura do protocolo) conforme mostra a figura abaixo:



CAMADA DE ACESSO À REDE

A camada inferior da arquitetura TCP/IP tem as funcionalidades referentes às camadas 1 e 2 do Modelo OSI.

Esta camada pode ser denominada, em outras literaturas, como Física ou até mesmo ser dividida em 2 camadas (Física e Enlace), o que leva a arquitetura a possuir 5 camadas.

CAMADA INTERNET

A camada Internet, também conhecida como de Rede ou *Internetwork*, é equivalente a camada 3, de Rede, do Modelo OSI. Os protocolos IP e ICMP(ping) estão presentes nesta camada.

CAMADA DE TRANSPORTE

A camada de Transporte equivale à camada 4 do Modelo OSI. Seus dois principais protocolos são o TCP e o UDP.

CAMADA DE APLICAÇÃO

A camada superior é chamada de camada de Aplicação equivalente às camadas 5, 6 e 7 do Modelo OSI. Os protocolos mais conhecidos são: HTTP, FTP, Telnet, DNS e SMTP.

EXERCÍCIOS PROPOSTOS

1. Defina uma rede de computadores.
2. Faça um esquema em diagrama de blocos que represente o processo de comunicação por rede e caracterize cada um dos blocos.
3. Faça o levantamento do hardware e software de rede.
 - 3.1. Crie uma folha de cálculo com o preço e as características técnicas de cada um dos componentes.
 - 3.2. Acrescente à folha de cálculo as características do software de rede, os requisitos mínimos e o respetivo preço.
4. Qual é a diferença entre transmissão em série e transmissão em paralelo? Faça um esquema.
5. Caracterize a transmissão em paralelo referindo as suas vantagens e desvantagens.
6. Caracterize uma transmissão em série.
7. Numa transmissão em série, o que entende por start bit, bit de paridade e stop bit.
8. O transporte de informação ao longo dos canais de comunicação é feito de três formas distintas. Caracterize cada uma das formas de transmissão, a seguir, mencionadas.

8.1. Simplex

8.2. Half-Duplex

8.3. Full-duplex

9. Qual é a diferença entre os seguintes tipos de transmissão:

9.1. difusão e ponto a ponto;

9.2. baseband e broadband;

9.3. síncrona e assíncrona.

10. Caracterize os seguintes tipos de transmissão wireless:

10.1. Infravermelhos

10.2. Ondas de rádio

10.3. Micro-ondas

11. Considera pertinente que o ser humano dê tanta importância à informação? Justifique.

12. Comente a afirmação: A qualidade da informação tornou-se prioritária em relação à quantidade de informação."

13. Qual pode ser o perigo de excesso de informação e da concorrência entre os vários meios de divulgação da informação?

14. Porque meios pode a informação ser divulgada?

15. Comente a afirmação: "Existem vários tipos de informação."

16. Indique uma ou mais razões que levam o computador a ser uma das ferramentas mais usadas no tratamento da informação.

17. Indique, em poucas palavras, em que consiste a informação digital.

18. O que é, basicamente, um código binário?

19. Comente a afirmação: "Apenas existe um sistema de numeração."

20. Comente a afirmação:

"Apesar de a numeração binária dispor apenas de dois algarismos (0 e 1), podemos utilizar vários *bits* e obter mais combinações diferentes."

21. Faça uma correspondência entre os oito primeiros números em decimal e binário (0-7).

22. Mostre como calcular o valor máximo que pode ser armazenado em:

22.1. KB

22.2. MB

22.3. GB

22.4. TB

22.5. PB

23. Comente a afirmação:

"O computador consegue entender um número decimal ou uma letra, mas não realiza as operações de adição, subtração, multiplicação e divisão no sistema binário."

24. O que é um octeto de bit?

- 25.** Faça uma apresentação em PowerPoint® ou no OpenOffice Impress subordinada ao tema:
"Importância da rede de dados."
- 26.** Inclua na apresentação os seguintes aspetos:
- 26.1.** Evolução das redes de comunicação;
 - 26.2.** Perspetivas de evolução das redes;
 - 26.3.** Áreas de aplicação das redes;
 - 26.4.** Redes ubíquas.
- 27.** Qual a diferença entre um sinal analógico e um sinal digital? Faça um esquema representativo.
- 28.** O que entende por largura de banda numa transmissão?
- 29.** Qual a unidade de largura de banda e os seus múltiplos?
- 30.** Qual a diferença entre largura de banda analógica e largura de banda digital?
- 31.** Quais as unidades de medida associadas aos dois tipos de largura de banda?
- 32.** Na medição da largura de banda, analógica ou digital, existem alguns fatores que têm de ser considerados. Enumere-os.
- 33.** De que forma os aspetos enumerados anteriormente. influenciam a largura de banda?
- 34.** Faça uma apresentação em PowerPoint® ou no OpenOffice Impress subordinada ao tema:
"Classificação de uma rede de computadores em função da distância, distribuição geográfica ou organizacional."

35. Faça uma apresentação em PowerPoint® ou no OpenOffice Impress ilustrando os seguintes meios de transmissão:

35.1. Cabos em par entrelaçado

35.2. Cabos coaxiais

35.3. Fibra ótica

35.4. Wireless

36. Descreva a utilidade de uma SAN [Storage Área Network] na rede de uma empresa.

37. Qual a diferença entre Intranet e Extranet?

38. Explique o motivo pelo qual existem normas e atividades de normalização de redes.

39. Quais os principais organismos de normalização?

40. Qual o papel de cada um dos organismos de normalização?

41. Indique as camadas definidas pelo modelo de referência OSI (MR-OSI). Explique, sucintamente, a finalidade de cada uma dessas camadas.

42. Descreva, resumidamente, o significado dos termos SDU, PCI e PDU utilizados no MR-OSI.

43. Qual é a importância do QoS entre camadas, no MR-OSI?

44. O padrão IEEE 802.3 descreve a tecnologia Ethernet.

44.1. Quais são as taxas de transmissão existentes numa rede Ethernet?

44.2. Caracterize as diferentes especificações da Ethernet a 10 Mbps.

45. Descreva, resumidamente, os padrões Token bus e *Token Ring*

46. Caracterize o padrão FDDI e o padrão IEEE 802.11 [wireless].

47. Em que consiste a comutação de pacotes?

47.1. O que são datagramas?

47.2. •Indique a diferença entre comutação de pacotes por circuito virtual e por datagramas.

48. Descreva a tecnologia ATM.

49. A arquitetura TCP/IP é desenvolvida em quatro camadas. Diga quais são e caracterize os serviços que oferecem.

50. Caracterize os diferentes protocolos/tecnologias de rede de camada TCP/IP:

50.1. SMTP, DNA, NSP, HTTP, FTP, TELNET;

50.2. TCP, UDP;

50.3. ICMP, IP, ARP, RARP;

50.4. ETHERNET, ATM, TOKEN RING.

51. Caracterize os protocolos IPX/SPX.

52. Quais as principais tarefas de um computador em rede?

53. Caracterize as principais funções dos seguintes servidores de rede:

53.1. Servidor de ficheiro

53.2. Servidor de impressora

53.3. Servidor de email

53.4. Servidor de DNS

53.5. Servidor de DHCP

53.6. Servidor de streaming

REFERÊNCIAS

Moreira, A. (s.d.). *Arquiteturas de Rede*. Obtido de

<https://www.dei.isep.ipp.pt/~asc/doc/arquitecturas.html>

Sá, J. P., Carvalho, R., & Silva, T. C. (2013). *Comunicação de Dados - Ensino Profissional Técnico de Gestão de Equipamentos Informáticos, Módulo1-2-3-4*. Porto: Porto Editora.

[Redes de comunicação em RS 485](#)

[Ligação lógica – controlo de fluxo e erros](#)