Escola Secundária da Moita

CEF – Curso de Educação e Formação

Manual de Redes

Curso de Instalação e Manutenção de Sistemas Informáticos

11º Ano

Gestão de Redes de Internet e Intranet

Ivan Franco
Nº 2 11º F2

4/5/2007

Índice

História das telecomunicações

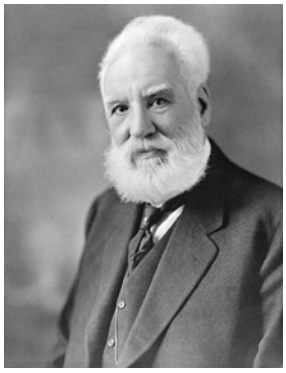
Nos tempos primitivos o homem comunicava por: gestos, sons. As primeiras comunicações eram: os pombos correio, sinais de luz, sinais de fumo.

Inicialmente, havia necessidade de comunicação, mas nada como hoje. Havia necessidade dessa comunicação por estarem em grupos juntos, mas há medida que se vão afastando, começam a existir outros tipos de comunicação.

Primeiro método de comunicação a ser utilizado (eléctrico) em larga escala foi o telégrafo. Foi inventado em 1837 por Morse. Utilizava o código com o nome do seu inventor para transmitir a informação. No entanto, era melhor para o homem poder comunicar pela voz, do que por código. Em 1876, Alexander Bell regista a patente do telefone.

Historicamente é considerado o inventor do telefone. Contudo existem indícios que apontam como legítimo inventor Antonio Meucci.

Bell nasceu em Edimburgo, Escócia. Veio de uma família ligada ao ensino de elocução: o seu avô em Londres, seu tio em Dublin, e seu pai, Sr. Alexander Melville Bell, em Edimburgo, eram todos elocucionistas professados. Este último publicou uma variedade de trabalhos sobre o assunto, dos quais vários são bem conhecidos, em especial o seu tratado na linguagem gestual, que apareceu em Edimburgo em 1868. Neste explica o seu método engenhoso de instruir surdos-mudos, por meio visual, como articular palavras e como ler o que as outras pessoas dizem pelo movimento dos lábios.



História das telecomunicações (continuação)

Graham Bell, seu filho distinto, foi educado na escola real de Edimburgo, onde se graduou aos 13 anos. Aos dezasseis fixou uma posição como professor de elocução e de música na academia de Weston House, em Elgin, Escócia. O ano seguinte foi passado na universidade de Edimburgo. De 1866 a 1867 foi instrutor na universidade de Somersetshire em Bath, Inglaterra. Enquanto esteve na Escócia virou a sua atenção para a ciência da acústica, com o objectivo de melhorar a surdez de sua mãe.

Em Portugal, a primeira comunicação telefónica foi realizada em 1877.
Tendo sido estabelecida pelo rei D. Luís I entre a povoação de Carcavelos e a estação do Cabo. Em 1901, Marconi demonstrou que as ondas de rádio podiam ser usadas para transmitir informação a longas distâncias. Exemplo: Inglaterra a França. A rádio é ainda hoje um dos métodos de transmissão, e é a base das telecomunicações móveis.

Foi em 1947 que inventaram o Transístor, foi esse o pequeno passo que proporcionou a revolução electrónica e a partir dai tem vindo a acontecer, e que forneceu a base para a rede telefónica computorizada, ao invés da mecânica.

Em 1965 Charles Kao avança com a teoria de que a informação pode ser transmitida por sinais luminosos, utilizando os cabos de fibra óptica. Esta teoria teve sucessivos desenvolvimentos até aos dias de hoje. De modo a facultar um meio de transmitir grandes quantidades de informação a taxas de transmissão bastantes altas.

Internet

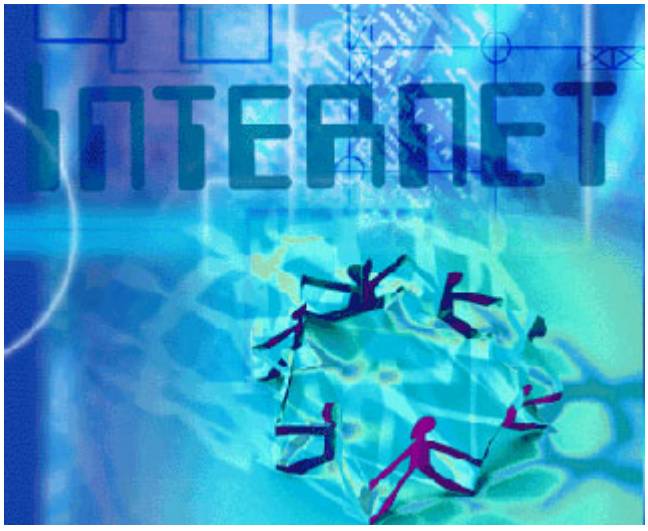
A Internet é uma rede de redes a nível mundial, de milhões de computadores. Com a Internet os computadores utilizam uma arquitectura de protocolos de comunicação TCP/IP. Permite transferência de arquivos, acesso remoto, e-mail, notícias e outros serviços.

A origem do nome surgiu de interligada (Inter), e network (net). A Internet é um sistema de informação global que é logicamente ligado por um endereço único global baseado no Internet Protocol (IP) ou as suas subsequentes extensões. È capaz de suportar comunicações usando o Transmission Control Protocol/Internet Protocol (TCP/IP), já referido, ou suas extensões e/ou outros protocolos compatíveis com o IP.

A Internet como rede mundial de computadores interligados, é um privilégio da vida moderna, para o homem moderno. È o maior reservatório de informações acessíveis a qualquer pessoa, que queira aceder em qualquer lugar do planeta.

World Wide Web

A World Wide Web - "a Web" ou "WWW" é uma rede de computadores na Internet que fornece informação em forma de hiper texto. Para ver a informação, pode-se usar um software chamado navegador para descarregar informações (chamadas "documentos" ou "páginas") de servidores de Internet (ou "sites") e mostrá-los no ambiente de trabalho do utilizador.



Intranet

A Intranet é uma rede de computadores privada que utiliza as mesmas tecnologias que a Internet. O protocolo de transmissão de dados da Intranet é o TCP/IP e sobre ele podemos encontrar vários tipos de serviços de rede comuns na Internet, como por exemplo o e-mail, chat, grupo de notícias, HTTP, FTP entre outros.

Rede interna de uma organização que utiliza a tecnologia Internet para permitir a partilha, o uso e a pesquisa de informação. As organizações utilizam as Intranets como um portal interno para comunicar com os seus funcionários e fornecer-lhes a informação que necessitam para o seu trabalho, com acesso restrito.

Tipos de Redes

56 Kbs Modem – Redes Telefónicas

- Analógica (56k) fixa
- RDIS (108k +- 112 k)

- Redes Moveis

- 2ª G (GSM) 9,6kbs
- 3ª G (UMTS) 115kbs

- Redes de dados

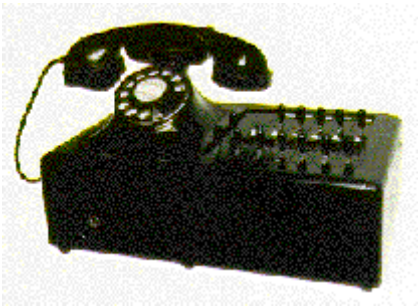
- TCP/IP
- ATM

- Redes de TV Cabo

Redes telefónicas:

A conexão pode ser realizada até uma taxa de 128Kbps, através de duas linhas de até 64 Kbps, que são usadas tanto para conexão com a Internet quanto para chamadas telefónicas de voz normais. É possível efectuar a conexão em apenas 64Kbps e deixando a outra linha disponível para chamadas de voz. Caso esteja conectado a 128 Kbps, ou seja, usando as duas linhas, não será possível realizar ou receber chamadas telefónicas. É possível também fazer duas chamadas telefónicas simultâneas, cada uma usando uma linha de 64 Kbps.

Esta taxa 128Kbps ocorre pelo fato da comunicação com a central telefónica ocorra de forma digital em todo o percurso, ao invés de forma analógica. Isto é explicado da seguinte forma: a largura de banda de uma linha analógica comum é de 4KHz, e em uma linha ISDN este valor é de 128Kbps, fazendo com que os 4KHz de sinal não existam mais, pois a linha conectada com a central de telefonia não trabalha com sinais analógicos.

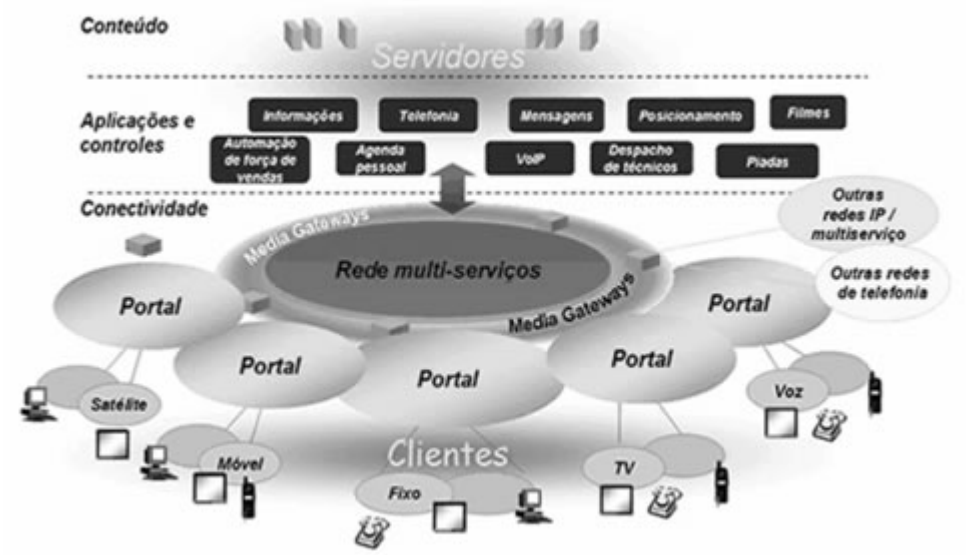


Redes Moveis:

2ª G- GSM (Global System for Mobile Communications, ou Sistema Global para Comunicações Móveis) é uma tecnologia móvel e o padrão mais popular para celulares do mundo. Telefones GSM são usados por mais de um bilhão de pessoas em mais de 200 países. A omnipresença do sistema GSM faz com que o roaming internacional seja muito comum através de "acordos de roaming" entre operadoras de celular. O GSM diferencia-se muito de seus predecessores sendo que o sinal e os canais de voz são digitais, o que significa que o GSM é visto como um sistema de celular de segunda geração (2.5G). Este fato também significa que a comunicação de dados foi acoplada ao sistema logo no início. GSM é um padrão aberto desenvolvido pela 3GPP.

3ª G- UMTS (acrónimo de Universal Mobile Telecommunication System) é uma das tecnologias de terceira geração (3G) dos telemóveis. O termo é adoptado para designar o padrão de 3ª Geração estabelecido como evolução para operadoras de GSM e que utiliza como interface rádio o WCDMA ou o EDGE.

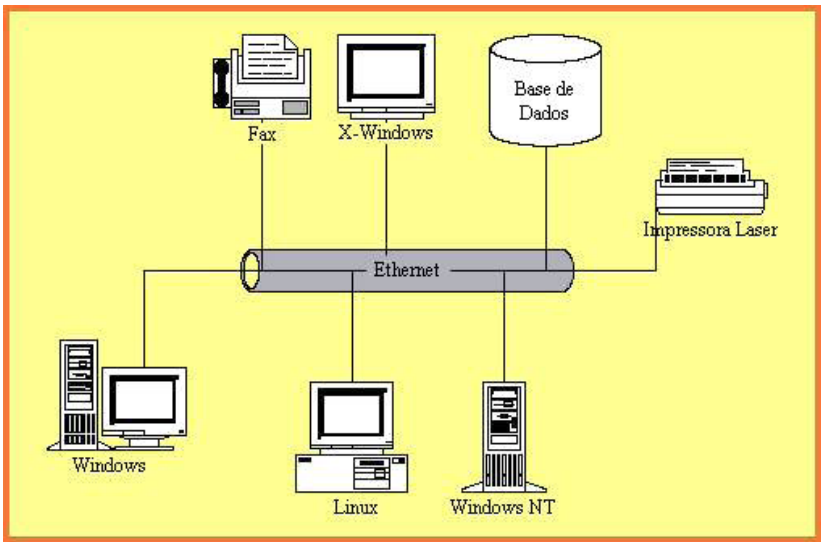
Até o ano de 2000 o desenvolvimento de padrões para o GSM foi conduzido pelo European Telecommunications Standards Institute (ETSI). A partir desta data a responsabilidade passou a ser do 3rd Generation Partnership Project (3GPP), que é um esforço conjunto de várias organizações de standards ao redor do mundo para definir um sistema celular global de 3º Geração UMTS (Universal Mobile Telecommunications System).



Redes de Dados:

TCP/IP- O modelo TCP/IP - como muitos outros modelos de protocolos - pode ser visto como um grupo de camadas, em que cada uma resolve um grupo de problemas da transmissão de dados, fornecendo um serviço bem definido para os protocolos da camada superior. Estas camadas mais altas estão logicamente mais perto do usuário (camada de aplicação), lidam com dados mais abstractos e confiam nos protocolos das camadas mais baixas para traduzir dados em um formato que pode eventualmente ser transmitido fisicamente.

ATM- O ATM é um protocolo de comutação rápida, que foi concebido no sentido do mesmo comutador ter capacidade para comutar todos os tipos de serviço oferecidos pela rede.



Redes de TV Cabo:

Redes TV cabo podem ser uni ou bi direccionais. As mais desinibidas são as unidireccionais, são mais baratos e não é necessário ter informação retorno.
Os canais de televisão fazem uso da chamada banda directa situada entre os 111 e 750 MHz, embora essa banda nas redes mais modernas possa ir até 1 GHz.

Classificação de redes

Uma rede de computadores consiste na interligação de diversos computadores, dispositivos periféricos e outros sistemas informáticos, com o objectivo de proporcionar uma melhor comunicação, organização e partilha de recursos existentes. É caracterizada pela sua extensão, abrangência e tecnologia de transmissão, bem como as características internas tais como, debito, meio de transmissão usado, topologia, nº máximo de dispositivos de rede.

- Lan
- Man
- Wan

Classificação de redes	Área	Velocidade	Fiabilidade	Responsabilidade
Lan	Pequena <1km	Muito alta	Grande	Utilizador
Man	Media <10km	Alta	Grande	Repartida entre o utilizador e fornecedor de serviço
Wan	Grande	Baixa	Baixa	Fornecedor de serviços

Lan:

As redes de área local são de pequena dimensão. Com a sua dimensão é conseguido um alto débito de dados. São muito fiáveis. O objectivo desta rede esta no aumento de produtividade e de eficiência dos utilizadores, reduzindo custos através da partilha de recursos, facilidade e rapidez na comunicação e organização interna.

A Lan utiliza o modelo cliente-servidor (fornece serviços ou seja, atende os pedidos, processa e responde). Servidor de impressoras; servidor de ficheiros; servidor de base de dados; servidor de Internet.

Man:

Estas redes não são mais alargadas que as Lan. A tecnologia usada é a mesma. A sua utilização esta na interligação numa área geográfica que não é maior que uma cidade. A velocidade de transmissão de dados é equivalente aos das redes locais, de modo a evitar o congestionamento.

Wan:

Este tipo de rede abrange uma grande área geográfica como cidades, países, continentes. Consiste numa série de dispositivos especializados que permitem a interligação de todos os outros computadores e redes. A velocidade de transmissão de dados é muito baixa quando comparada com as redes antes mencionadas.

Topologias de Rede

- Barramento (todos os elementos utilizam o mesmo meio de comunicação)

- Anel (consiste em ligação ponto-a-ponto entre dispositivos que formam um circulo fechado)

- Estrela (todos os elementos da rede estão ligados a um ponto central)

- Arvore (é designada por topologia hierárquica)

- Não constrangida (são denominadas por híbridas)

Não Constrangida

Também denominadas de híbridas, não têm nenhuma configuração definida. Os elementos estão ligados entre si ponto a ponto de uma maneira arbitrária, que varia grandemente de uma implementação para a outra.

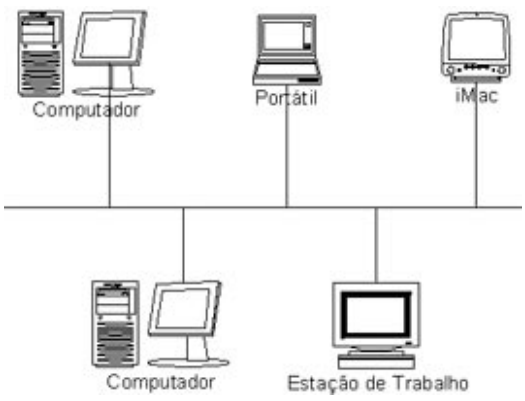
Os problemas de roteamento associados com estas redes são bastantes difíceis de resolver. Os elementos que efectuam o roteamento, por vezes têm de executar outro tipo de funções relacionadas com a rede. Introduz atraso e adiciona carga indesejada.

Constrangida:

Barramento

Todos os elementos da rede partilham o mesmo meio de transmissão. Apenas um par de elementos pode estar a comunicar simultaneamente. Quando um pacote de dados é transmitido, propaga-se a todos os elementos da rede, sendo recebido por todos.

As vantagens são que, como o tamanho dos cabos é menor que nas outras topologias, os barramentos são ideais para protocolos que usem método de contenção. São também fáceis de reconfigurar, adicionando ou eliminando utilizadores e o meio de transmissão é fiável.



Anel

Consiste em ligações ponto-a-ponto entre pares de dispositivos que no seu conjunto formam um círculo fechado.

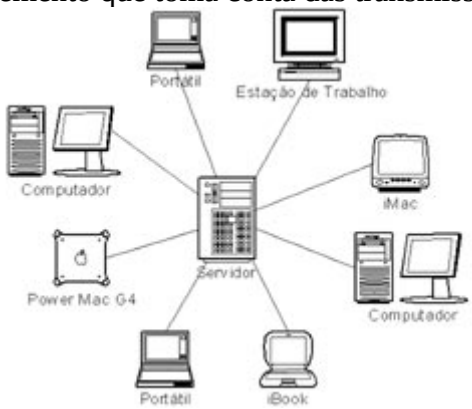
A informação é transmitida através do anel sob a forma de um pacote de dados que é enviado rotativamente segundo uma direcção predefinida. A informação é assim enviada para cada um dos elementos da rede, e depois reenviada, até ser retirada.
Basta um nó não estar ligado e o circuito fica interrompido.

Estrela

Todos os elementos da rede estão ligados a um ponto central, também denominado por Hub. O ponto central pode ser activo ou passivo.

A grande vantagem reside no facto de poder ser expandida muito facilmente.

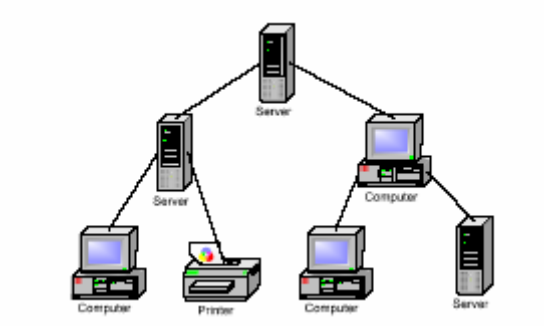
O aumento de elementos na rede pode ir, teoricamente, até ao infinito. As técnicas de acesso à rede são mais fáceis do que em qualquer das topologias anteriores, uma vez que existe um elemento que toma conta das transmissões na rede.



Árvore

É designada como topologia hierárquica, e tal como, o nome indica é estruturada em níveis. Tem algumas características como a de barramento e em estrela.

O nível superior não é o único a tratar do endereçamento e gestão do fluxo da informação na rede. A informação é transmitida por um dispositivo num nível mais baixo só recua o suficiente até trocar de segmento de rede para chegar ao seu destino, podendo nem passar pela raiz.



Transmissão de Informação

A informação produzida por uma determinada frente seja ela sonora, visual, informática, pode ser convertida num sinal electromagnético. Esta informação é então colocada num meio de transmissão e é propagado desde o emissor até ao receptor.

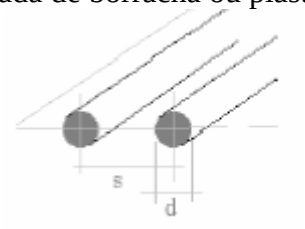
Meios de Transmissão

O meio de transmissão é a ligação física, pela qual se propagam as ondas, entre o emissor e o receptor num sistema de emissão de dados.

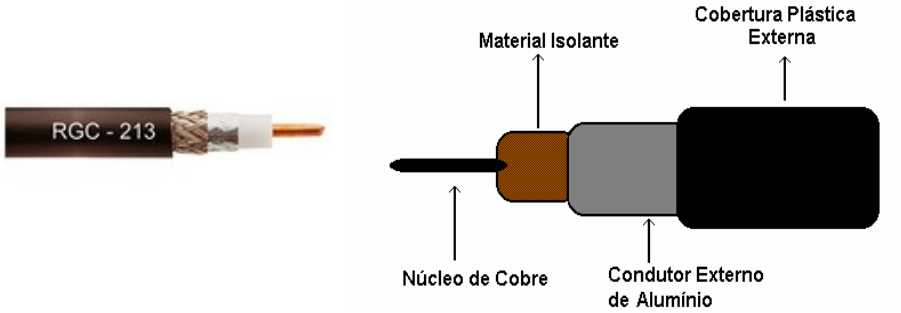
Meios Guiados

- Linha Bifilar
- Cabo Coaxial
- Par Entrançado
- Fibra Óptica
- Guia de Planos Paralelos
- Guia Cilíndrico
- Guia Paralelipipédico

Linha Bifilar → é composta por dois condutores paralelos, geralmente em forma cilíndrica envoltos por uma camada de borracha ou plástico isolante.



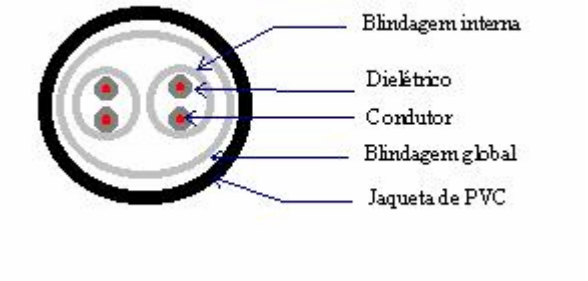
Cabo Coaxial → é constituído por um núcleo de cobre envolvido por um material isolante. O núcleo é usado para transportar dados, enquanto que o condutor externo serve como escudo e protege o princípio de interferências externas. Existem dois principais variantes destes cabos: Baseband e Broadband.
O cabo coaxial baseband é usado para transmissões digitais entre grandes distâncias. Um cabo coaxial com 500m permite um débito máximo de 1Gigabit(seg).
Tecnicamente, o cabo coaxial broadband é considerado de qualidade inferior ao cabo baseband na transmissão de dados, mas tem a vantagem de já estar instalado por todo o lado.



Desvantagens: vulgar, que os terminais e as fichas que são ligadas apresentam maus contactos após pouco tempo de utilização, o que vai provocar interferências e diminuir a qualidade de transmissão.

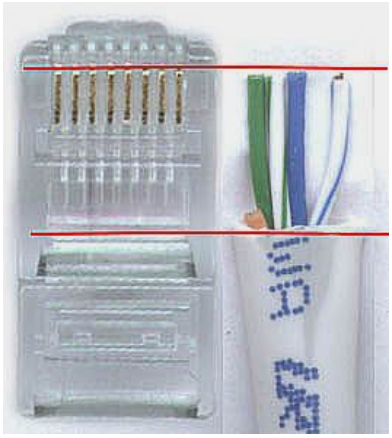
É utilizado em tipologias "Barramento".

Par Entrançado → este suporte físico consiste em pares de fios de cobre isolados e entrançados entre si, protegidos por uma camada isolante. A transmissão analógica e digital é conseguida com débitos que dependem do cabo utilizada e da distância percorrida, obtendo-se em média vários MegaBits/seg entre poucos quilómetros.



Desvantagens: Distância Máxima.

Ficha RJ45 → é bastante barato e o facto de ser maleável torna-o ideal para instalações em prédios. A desvantagem prende-se com a distância máxima sem amplificação.



Fibra Óptica → é similar em forma ao cabo coaxial. Consiste num núcleo de fibra de vidro denominado "Core" onde os dados são propagados sob a forma de luz, envolvido por outra camada de fibra de vidro (cladding). É comum em sistemas que requerem altos débitos, o agrupamento de várias fibras ópticas num só cabo sob uma camada protectora.

Vantagem: Grandes distâncias.
Desvantagem: preço, fragilidade.

Meios Não Guiados

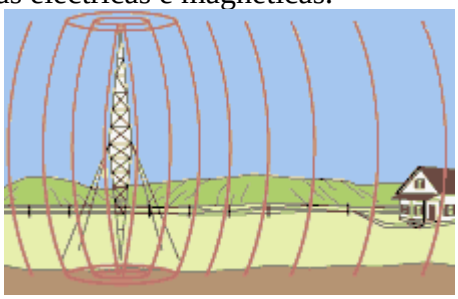
São caracterizados por não conduzirem as ondas electromagnéticas. São meios de propagação das ondas, mas não têm uma direcção predefinida.

Utilizam outros métodos de transmissão que são denominados por Wireless:

- Ondas Rádio;
- Infravermelhos;
- Micro-ondas (Bluetooth, Ligações Terrestres e Ligações Terra-Satelite);
- Laser.

Ondas Rádio

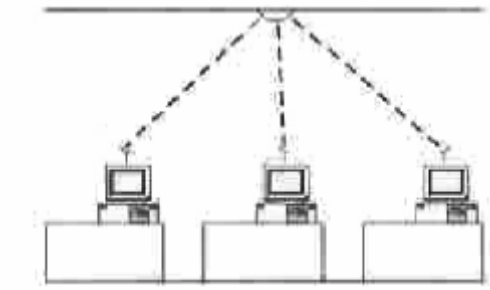
São muito usadas na comunicação porque são fáceis de gerar, propagam-se em todos os sentidos. Os seus problemas estão numa dependência da frequência utilizada. No entanto, as ondas de rádio não são um meio fiável de transmissão, pois são bastante susceptíveis a interferências eléctricas e magnéticas.



Infravermelhos

O mais comum exemplo será através dos comandos remotos de televisão, vídeo, etc. tem um baixo custo e facilidade de construção, mas pecam por não poderem atravessar grande parte dos materiais.

Os infravermelhos funcionam com base em códigos abertos utilizados pelos vários fabricantes de aparelhos electromagnéticos. Na transferência de dados é utilizado também um protocolo especial criado para o efeito.



Micro-ondas

Não são mais que ondas electromagnéticas, mas que trabalham em frequências muito superiores.

É muito usado na comunicação telefónica entre grandes distâncias. É barata e fácil de implementar, pois basta construir uma torre de transmissão para transmitir a informação num raio de 50km.

Bluetooth: é um caso particular das micro-ondas. Trata-se de um protocolo de comunicação via ondas de rádio, mais precisamente micro-ondas, de alto alcance e baixa potência. Funciona nos 2.4GHz e tem um alcance de cerca de 10 metros.

Ligações Terrestres

As ligações terrestres são utilizadas na interligação de redes privadas, desde que exista linha de vista entre os locais a interligar. É usual em utilizações até aos 3 km, suportando débitos de 2 ou 10 Mbps. É também possível, ligações até aos 50 km, sendo, para isso necessário, a utilização de potenciadores nos transmissores. Estes potenciadores são somente autorizados a operadores de telecomunicações.

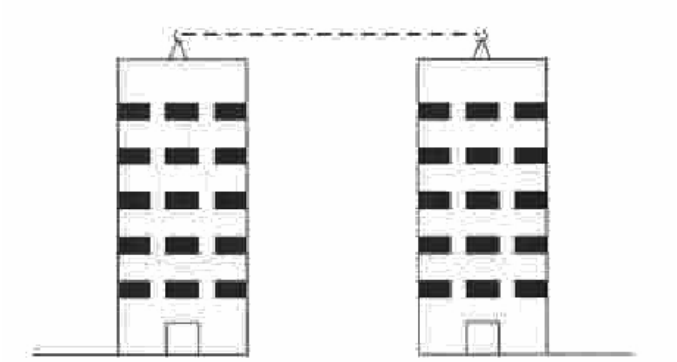
Ligações Terra-satélite

As **ligações terra-satélite** são normalmente utilizadas nas intercontinentais das redes dos operadores de telecomunicações, sendo também usual a utilização deste tipo de ligações em redes informáticas com elevada dispersão geográfica ou localizadas em locais remotos. A largura de banda suportada por este tipo de ligações é bastante elevada, na ordem dos 500MHz, sendo normal, atrasos também bastante grandes, na ordem dos 0,25 segundos em ligações geostacionárias, podendo ser perturbadores em aplicações interactivas.

Ligações Laser

As emissões laser podem ser utilizadas para transportar informação num espaço aberto desde que exista linha de vista entre os dois pontos. Este tipo de ligações para interligar redes privadas nas situações em que exista linha de vista entre os pontos a interligar, não é possível ou economicamente rentável a instalação de cabos de fibra óptica.

A sua principal vantagem reside na enorme largura de banda disponível (622 Mbps a distâncias na ordem dos 3 km) e no facto de não existir necessidade de obter aprovação das entidades gestoras do espaço radioeléctrico para a instalação das ligações. A sua principal desvantagem está relacionada com a sua enorme sensibilidade ás condições atmosféricas, nomeadamente a existência de nevoeiros ou poeiras no percurso do feixe. Outra desvantagem importante está relacionada com a necessidade de se manter uma alinhamento rigoroso aos dispositivos emissor e receptor, o que poderá ser complicado de manter quando a distância aumenta e quando se tem que fazer recurso a torres metálicas ou de outras estruturas sensíveis aos ventos ou à dilatação térmica.



Largura de Banda

O significado de largura de banda varia com o contexto em que é utilizado. Ao analisarmos um sinal representado em frequência, vemos que existem frequências em que a amplitude é significativa. À diferença entre a frequência máxima e a frequência mínima que compõem um sinal, seja ela analógico ou digital, chama-se **largura de banda**.

Ora, se representarmos graficamente a largura de banda, observamos uma espécie de janela. Quanto maior for essa janela, mais informação consegue transportar, ou seja, mais dados cabem pela janela. Assim, o conceito de largura de banda em redes de computadores, e em geral, a sinais **digitais**, corresponde à quantidade de dados enviados por unidade de tempo num determinado canal de comunicação.

Em termos físicos, estamos na realidade a falar da capacidade do canal, ou seja, a quantidade de símbolos que conseguimos transmitir, dada a largura de banda de determinado canal.
Este significado é o mesmo que ritmo de transmissão em que a largura de banda para sinais digitais será o ritmo binário máximo que se poderá atingir em determinado canal de comunicação.

A origem dos números

No sistema de numeração utilizado no dia a dia, usamos um sistema com dez símbolos para representar os números existentes. Esses símbolos vão de 0 a 9 e representam o sistema de numeração decimal, precisamente por conter 10 símbolos diferentes, denominados algarismos. Para os números superiores a 9 é usada uma convenção de escrita, que atribui um significado diferente ao local onde é colocado o novo dígito.
Por exemplo, em virtude das posições ocupadas o número 6903 tem um significado numérico calculado da forma:

$$6903 = 6 \times 1000 + 9 \times 100 + 0 \times 10 + 3$$

Ou colocando sob a forma de potências de 10:

$$6903 = 6 \times 10^3 + 9 \times 10^2 + 0 \times 10^1 + 3 \times 10^0$$

Reparamos que o número é a soma de potências de 10 multiplicadas por um coeficiente apropriado. Uma vez que a base da potenciação é o número 10, dizemos que estamos em presença de um número representado na base 10 ou decimal.
Ora, o facto mais atraente é que não existe nada que force o ser humano a usar dez algarismos diferentes para representar um número. O nosso sistema de numeração decimal cresceu devido ao facto de possuirmos 10 dedos.
Podemos ter uma base numérica de qualquer valor. Utilizando um sistema em que a base fosse *n*, haveria *n* símbolos representando algarismos, sendo o mais elevado de valor *n-1*.

Bases Numéricas

É verdade que podemos ter bases numéricas de qualquer valor. No entanto, tal não se justifica a não ser que realmente estejamos interessados em ser diferentes do resto da humanidade. Existem, no entanto, algumas bases numéricas bastante utilizadas e divulgadas.

Base Octogonal

Como o próprio nome indica, a base octogonal utiliza o 8 como raiz. Existem, assim, 8 algarismos diferentes, que variam desde o 0 até ao 7. A representação do número 8 será então 10o, e assim sucessivamente. A base octogonal utiliza-se na representação de sistemas de numeração de computadores, e em programação de sistemas informáticos.

Base Hexadecimal

Hexadecimal quer dizer que possui 16 símbolos, ou algarismos, para a representação de números. Ora, nós conhecemos apenas 10 símbolos, os mesmos da numeração decimal. Então, por convenção, atribuíram-se mais 6 letras, de A a F para representar os algarismos que faltavam. Assim, e de acordo com a tabela, temos os valores dos algarismos hexadecimais e a sua correspondência na numeração decimal.

Digito	Valor
A	10
B	11
C	12
D	13
E	14
F	15

A numeração hexadecimal possui, assim, 16 algarismos, de 0 a F, e a raiz da Potenciação é o 16, à semelhança do que acontece com as outras bases já mencionadas. Os números escritos abaixo são exemplos de números hexadecimais:

12FFh
3EF4h
3456h
3000h

Como regra geral, e para distinguir a base hexadecimal das restantes, escreve-se a letra H junto ao número representado.

Base binária

A base binária, muito utilizada nos sistemas digitais, como o nome indica, contém apenas dois símbolos ou algarismos, o 0 e o 1. Da conjunção do termo em inglês *binary digit,* surgiu então a palavra BIT. Um bit é, nada mais, nada menos, que um dígito binário. Uma das vantagens da utilização de dígitos binários, ou bits, é a sua analogia directa com a lógica booleana. O dígito 1 corresponde a um verdadeiro, enquanto que o 0 corresponderá a um Falso.

Bytes

Um bit é raro aparecer sozinho. Os primeiros computadores a aparecer no mundo, trabalhavam com conjuntos de 8 bits. A este conjunto de 8 bits convencionou-se chamar byte[2]. À medida que os computadores iam evoluindo tecnologicamente, o conjunto de bits com que trabalhavam também o foi, aparecendo outros nomes para conjuntos de bits diferentes.

Número de Bits	Nome
4	Nibble
8	Byte
16	Word
32	Double Word
64	Long Word

Potenciação em base binária

Para um número em base natural que contenha 2 dígitos, podemos representar, com esses 2 dígitos 10_2 números diferentes. Ou seja, de 0 a 99, existindo 100 números diferentes. Com três dígitos poderemos representar 10^3 números, ou seja 1000 números diferentes, e assim sucessivamente. O mesmo acontece com as outras bases. Tomando como exemplo a base binária, com dois bits poderemos representar 2^2 números, ou seja, 4. Com três bits poderemos representar 2_3 números, ou seja 8. E assim sucessivamente. Com um byte, ou seja 8 bits, poderemos então representar 2^8 números. Fazendo as contas, obtemos 256 números diferentes, com apenas 8 bits. Assim, poderemos construir uma tabela de potenciação com os valores possíveis de obter em base binária, para determinado número de bits.

Número de bits	Potenciação	Quantidade
1	2_1	2
2	2_2	4
3	2_3	8
4	2_4	16
5	2_5	32
6	2_6	64
7	2_7	128
8	2_8	256
9	2_9	512
10	2_{10}	1024

Contagem de Bytes

Quando nos dirigimos a um ponto de venda de hardware, a quantificação da informação que pode ser guardada em disco ou em memória parece em bytes e não em bits. Como um byte é nada mais nada menos que 8 bits, a informação não deixa de estar correcta, uma vez que são raras as vezes em que um bit aparece sozinho. Assim, e à medida que aumentamos a quantidade de bytes, vamos utilizando prefixos, tal como utilizamos no sistema de base natural.

Nome	Abreviação	Tamanho
Kilo	K	2^{10} = 1,024
Mega	M	2^{20} = 1,048,576
Giga	G	2^{30} = 1,073,741,824
Tera	T	2^{40} = 1,099,511,627,776
Peta	P	2^{50} = 1,125,899,906,842,624
Exa	E	2^{60} = 1,152,921,504,606,846,976
Zetta	Z	2^{70} = 1,180,591,620,717,411,303,424
Yotta	Y	2^{0} = 1,208,925,819,614,629,174,706,176

Um CD leva cerca de 650/700 Megabytes. Nos dias que correm, os discos são da ordem dos Gigabytes. Bases de Dados com alguns Terabytes de informação existem por esse mundo fora, enquanto que talvez apenas as bases de dados do FBI ou do Pentágono suportem alguns Petabytes de dados.

Modos de Transmissão

Transferência de dados série e paralelo

Os 2 principais modos de transferências de dados são o modo paralelo e modo série. O modo paralelo tem como característica a transferência paralela de um byte de dados, ou seja, os 8 bits que compõem o byte são transferidos todos de uma só vez através de uma pluralidade de linhas de comunicação. Assim, para a transferência paralela de 8bits são precisas 8 linhas de transmissão.

No modo série, os bits que compõem um byte de dados, são enviados sequencialmente através de uma única linha.

No modo paralelo estão cada vez mais em desuso. Praticamente nos dias que correm apenas são usados entre um computador e uma impressora.

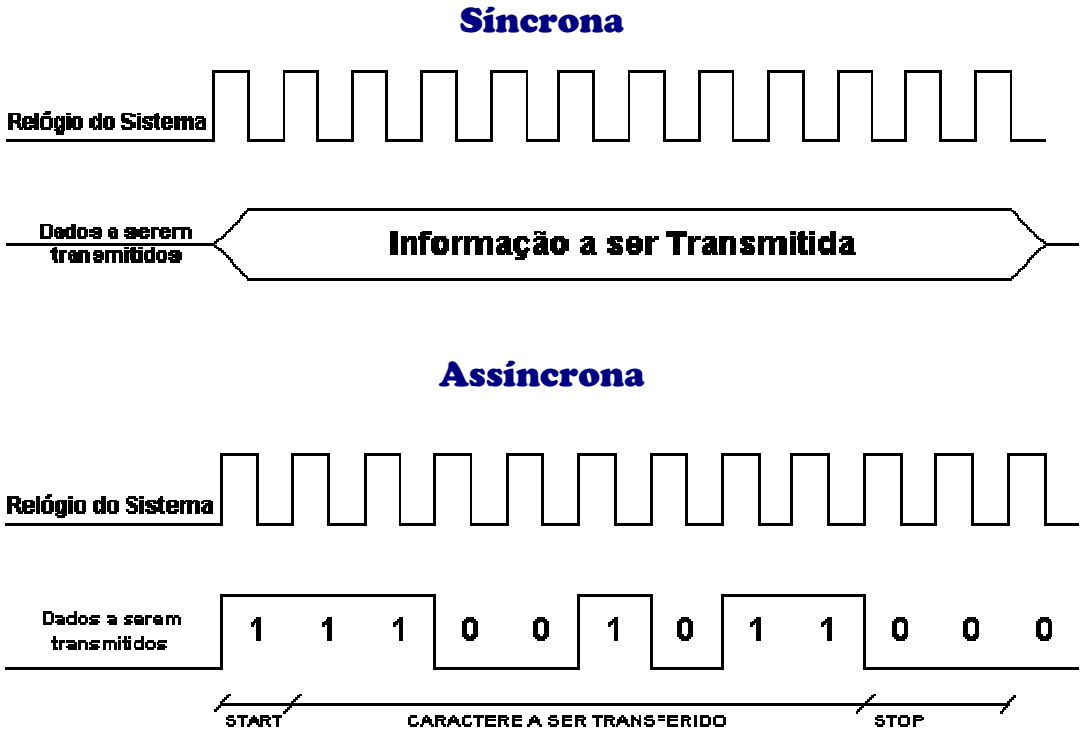
Transmissão em série - em que os dados são transmitidos bit a bit, uns a seguir aos outros, sequencialmente (como acontece, por exemplo, entre a porta série de um computador e um *Modem* externo);

Transmissão em paralelo - em que são transmitidos vários bits ao mesmo tempo (por exemplo, 8 bits em simultâneo, como acontece entre uma porta paralela de um computador e uma Impressora).

Síncronos e Assíncronos

Dentro do modo de transmissão em série podemos ainda distinguir entre transmissão síncrona e assíncrona. A diferença entre eles é bastante simples: no modo síncrono um ou mais adicionais são transmitidos, que indicam quando é que o próximo bit é valido na linha de transmissão.
A vantagem da transmissão síncrona é o que o receptor responde a varias taxas de relógio.

No modo de transmissão assíncrona os bits de dados acomodam eles próprios informação de sincronização. Neste caso, o emissor e o receptor têm de operar à mesma frequência.



Paridade

A paridade, apesar de ser um método de verificação de erros, é bastante simples e ineficaz nessa função. A paridade apenas consegue detectar erros de um único bit. Se um sinal sofrer uma interferência que altere mais que um bit, a paridade não terá significado. É apenas útil em linhas de transferência curtas e pouco sujeitas a interferências.
A vantagem desta paridade, é que praticamente qualquer interface série suporta esta verificação, que sempre é melhor do que nenhuma.
Existem 5 paridades possíveis:

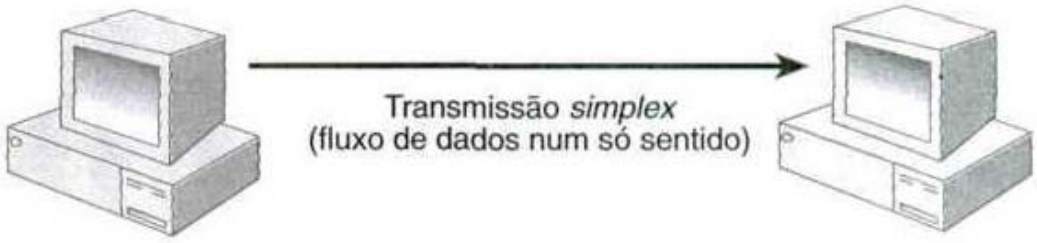
- Sem paridade;
- Par;
- Impar;
- Mark;
- Space.

As paridades Mark e Space são apenas úteis para detectar erros no próprio bit de paridade.

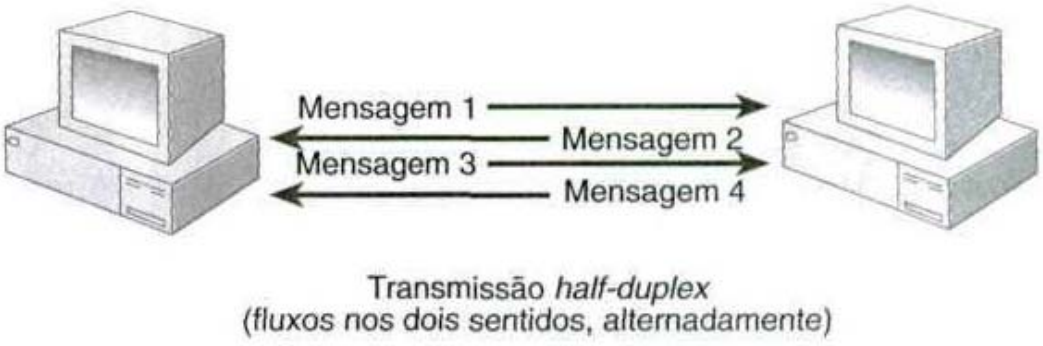
Modos de Comunicação

Quanto aos sentidos em que a informação pode ser transmitida através de um canal entre emissores e receptores, as transmissões de dados podem ser de três tipos:

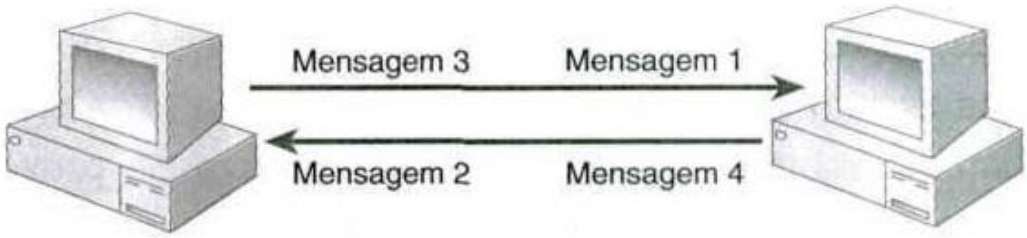
Simplex - neste caso, as transmissões podem ser feitas apenas num só sentido, de um dispositivo emissor para um ou mais dispositivos receptores; e o que se passa, por exemplo, numa emissão de rádio ou televisão; em redes de computadores, normalmente, as transmissões não são deste tipo.



Half-Duplex - nesta modalidade, uma transmissão pode ser feita nos dois sentidos, mas alternadamente, isto e, ora num sentido ora no outro, e não nos dois sentidos ao mesmo tempo; este tipo de transmissão e bem exemplificado pelas comunicações entre radioamadores (quando um transmite o outro escuta e reciprocamente); ocorre em muitas situações na comunicação entre computadores.



Full-Duplex - neste caso, as transmissões podem ser feitas nos dois sentidos em simultâneo, ou seja, um dispositivo pode transmitir informação ao mesmo tempo que pode também recebe-la; um exemplo típico destas transmissões são as comunicações telefónicas: também são possíveis entre computadores. Desde que o meio de transmissão utilizado contenha pelo menos dois canais, um para cada sentido do fluxo dos dados.



Transmissão *full-duplex*
(fluxos nos dois sentidos, simultaneamente)

Ligações de Acesso a Redes (Rede Internet)

Modems Analógicos

Um dispositivo que transforma os sinais digitais enviados e os modula em sinais analógicos; ele também transforma os sinais analógicos recebidos e os demodula em sinais digitais. Os modems analógicos têm sido utilizados para transmitir dados de um computador através de uma linha telefónica.

RDIS

RDIS (acrónimo para Rede Digital com Integração de Serviços), em inglês ISDN (*Integrated Service Digital Network*), usa o sistema telefónico comum. O ISDN já existe a algum tempo, sendo consolidado nos anos de 1984 e 1986, sendo umas das pioneiras na tecnologia xDSL.

A conexão pode ser realizada até uma taxa de 128Kbps, através de duas linhas de até 64 Kbps, que são usadas tanto para conexão com a Internet quanto para chamadas telefónicas de voz normais. É possível efectuar a conexão em apenas 64Kbps e deixando a outra linha disponível para chamadas de voz. Caso esteja conectado a 128 Kbps, ou seja, usando as duas linhas, não será possível realizar ou receber chamadas telefónicas. É possível também fazer duas chamadas telefónicas simultâneas, cada uma usando uma linha de 64 Kbps.

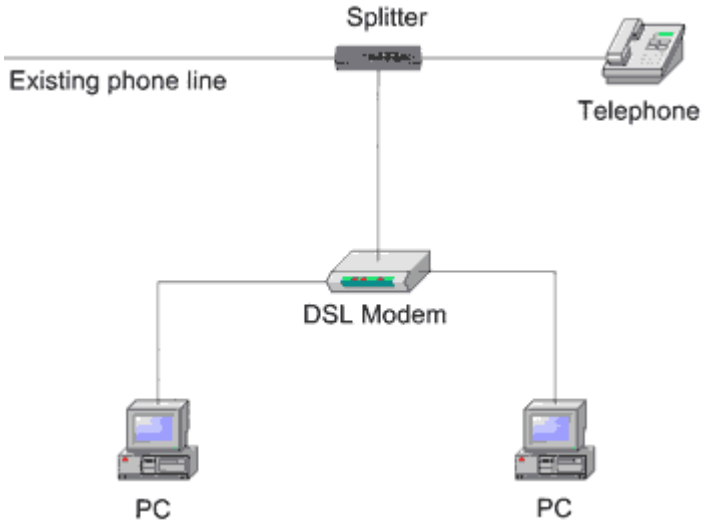
DSL

Digital Subscriber Line, ou simplesmente DSL, é uma família de tecnologias que fornecem um meio de transmissão digital de dados, aproveitando a própria rede de telefonia que chega na maioria das residências. As velocidades típicas de download de uma linha DSL variam de 128 kilobits por segundo (kbit/s) até 24 mil kbits/s dependendo da tecnologia implementada e oferecida aos clientes. As velocidades de upload são menores do que as de download para o ADSL e são iguais para o caso do SDSL.

As ligações DSL trazem algumas vantagens em relação as tradicionais por modem:

- Possibilidade de manter chamadas d voz enquanto se navega na Internet;
- A velocidade é muito maior que num modem tradicional;
- Não é necessária instalação de novos cabos.

A tecnologia DSL foi criada para tirar melhor partido da comunicação de dados sobre linhas de cobre, um suporte com mais de 100 anos de existência e ate à data bastante subaproveitada.

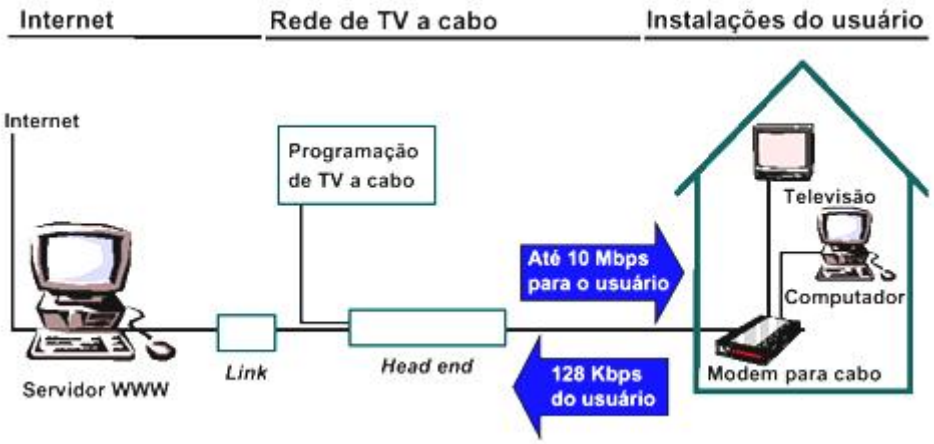


Internet por Cabo

A Internet via cabo permite que os assinantes acessem o conteúdo e serviços disponíveis diretamente na rede de alta velocidade, sem precisar passar pela conexão via telefone. Por isso, é necessário que o usuário seja assinante da TV a cabo, para poder acessar a rede em alta velocidade. A transmissão de dados é feita através de cabos de **fibra optica** (foto ao lado), que são, basicamente, fios de vidro ou de plástico que guiam sinais luminosos, circulares em sua secção transversal.

As vantagens da Internet via cabo são muitas, a começar pela qualidade de som e imagem superiores à conexão por telefone. Além disso, a velocidade vai de 128 Kbps, podendo chegar até 512 Kbps, ou seja, permite que os utilizadores tenham um melhor aproveitamento de diversos serviços oferecidos pela rede, como por exemplo, façam downloads de documentos com grandes extensões em poucos segundos. O serviço também é multiplataforma, quer dizer, está disponível para PC, Mac ou Linux, com total segurança através de programas de antivírus Norton.

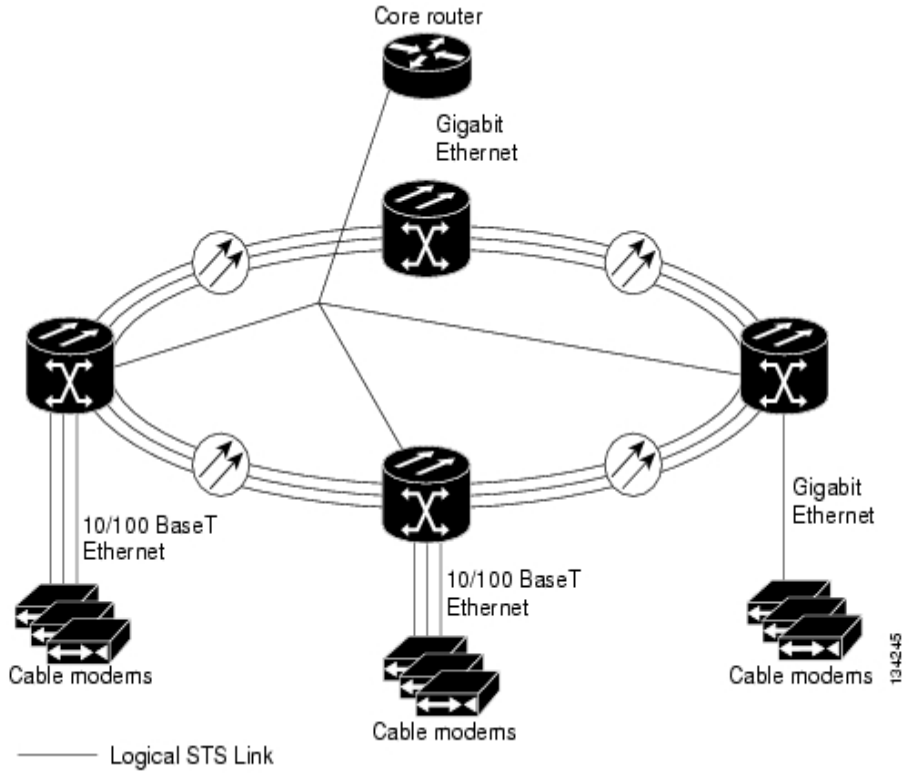
O acesso é 24 horas e isto significa que o utilizador está sempre conectado, podendo acessar a rede a qualquer momento, sem se preocupar com os gastos com impulsos telefónicos.



Modem por Cabo

Um modem por cabo pode ser externo ao PC ou interno, ou ainda estar integrado na set-top box da televisão por cabo. Em qualquer dos casos, é composto pelos componentes seguintes:

- Sintonizador (Tuner);
- Desmodulador;
- Modulador;
- Controlo de Acesso ao meio (MAC);
- Processador.



Sintonizador (Tuner): O sintonizador é conectado à saída de cabo que está na parede. Tem por função sintonizar o canal de dados, uma vez que este está colocado numa faixa de canais normais de televisão. Muitas vezes, o sintonizador inclui um *splitter* para separar o canal de dados dos canais de TV.

Desmodulador: Os desmoduladores mais comuns têm quatro funções. Um desmodulador de QAM é usado para obter os sinais de informação e convertê-los para um sinal que possa ser processado pelo conversor A/D. Contém ainda um módulo de correcção de erros, para que os bits, já depois de convertidos pelo conversor A/D possam ser comparados com um padrão predefinido, de modo a corrigir a informação, se necessário. Pode conter ainda um sincronizador de *frames*, que usa o padrão MPEG para o efeito, uma vez que os dados, tal como os sinais de TV são embutidos em *frames* MPEG.

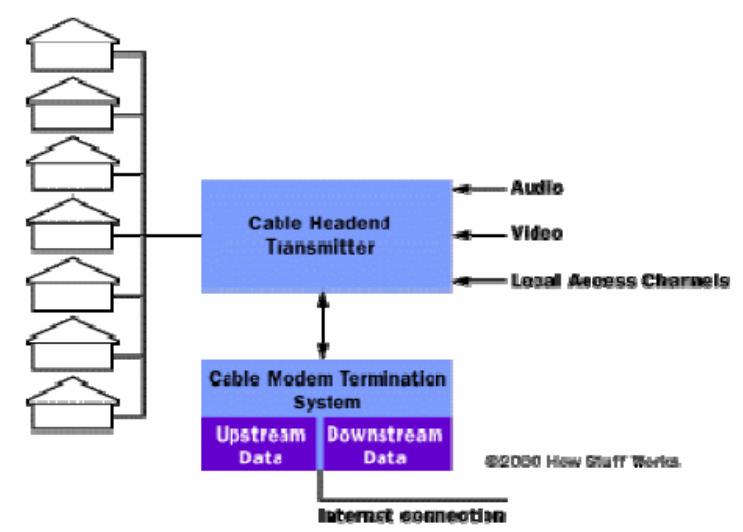
Modulador: Nos sistemas em que o upstream se faz pelo mesmo cabo, existe um modulador que converte os sinais digitais do computador em sinais de rádio frequência de modo a poderem ser transmitidos pela rede de televisão.

Controlo de Acesso ao meio (MAC): Situa-se entre as partes de downstream e de upstream do modem, e é responsável por servir de interface ao hardware e software dos diferentes protocolos de rede em coexistência no modem.

Processador: Este componente existe quando o modem faz parte de um sistema maior de computação, não servindo apenas de interface da Internet, ao que neste caso o processador seria o do próprio computador externo ao modem.

CMTS

No que respeita ao funcionamento, o CMTS é equivalente ao DSLAM num sistema DSL. O CMTS congrega o tráfego que chega de um grupo de utilizadores e transfere-o para uma linha de alto débito até ao ISP. O fornecedor do serviço por cabo terá servidores para autenticação e outras funções essenciais à ligação à Internet.



Um único CMTS na rede é suficiente para ligar cerca de 1000 utilizadores num único canal de 6 MHz, uma vez que cada canal destes tem uma capacidade de cerca de 40 Mbps. O único aspecto negativo prende-se com o facto desta largura de banda ser partilhada, o que, no caso de haver um número de utilizadores significativos no canal, leva à degradação da capacidade deste, o que em situações extremas pode ser bastante inferior à largura de banda contratada de cerca de 640 Kbps por utilizador. Geralmente esta situação ultrapassa-se facilmente com a inclusão de mais canais de 6 MHz para a transferência de dados.

A grande vantagem do cabo face ao DSL é que não depende da distância a que o utilizador está da central (CMTS), uma vez que o sistema de televisão por cabo é desenhado para providenciar sinais muito bons de transmissão.

Outras Tecnologias de Rede

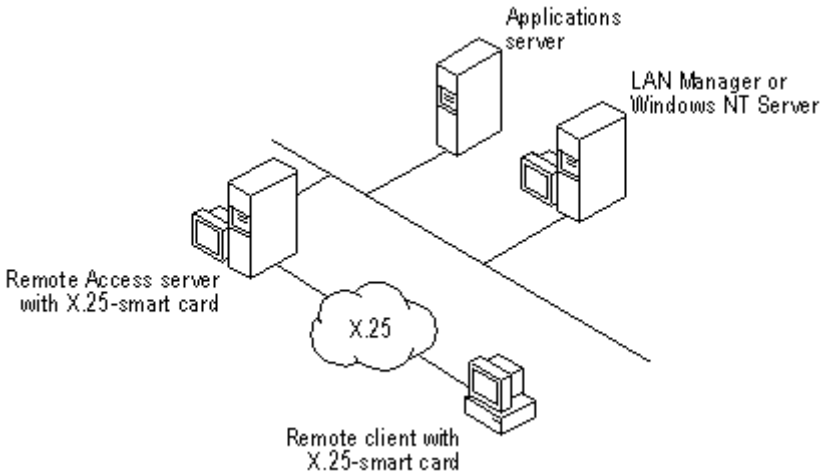
O utilizador final, quando se liga à Internet, fá-lo por uma ligação via linha analógica, DSL, RDIS, Modem por Cabo, PowerLine, etc. O tráfego dos vários utilizadores é congregado em centrais, quer sejam os próprios servidores dos ISPs, quer sejam centrais especiais, como no caso do DSL e do cabo, situadas a poucos quilómetros dos utilizadores. O tráfego é congregado e transferido para uma linha de alto débito, que se baseia em tecnologias diferentes das utilizadas pelo consumidor final, geralmente baseadas em fibra óptica.

No caso de se tratar de uma ligação de WAN, existem ainda outras tecnologias disponíveis para empresas que não ISP que variam de qualidade, fiabilidade e custo. Existem também outras tecnologias de acesso que não se baseiam em suportes materiais, mas sim em acessos via rádio. Estes trazem as vantagens associadas a sistemas *wireless*.

X.25

Nos anos 70 houve a necessidade de criar alguns protocolos de ligações WAN que funcionassem sobre a rede telefónica já existente. O X.25, desenvolvido pelas principais companhias telefonias mundiais, foi o protocolo que mais vingou. As suas especificações são desenhadas de modo a funcionar sob qualquer meio de transmissão. A grande vantagem do X.25 é a sua internacionalização, uma vez que o protocolo é regulado pelas entidades internacionais.

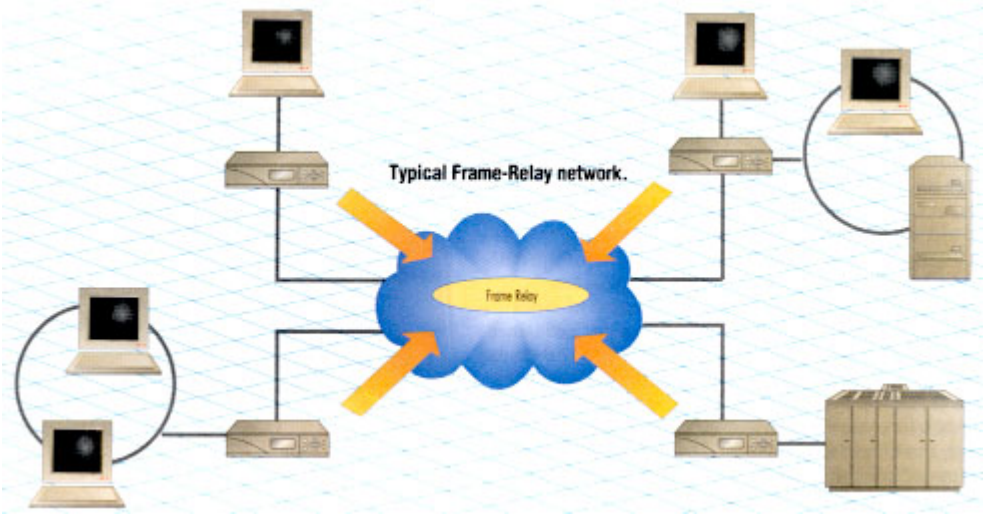
Apesar dos seus ritmos de transmissão muito baixos, na ordem dos 64 kbps, e a sua elevada latência, na ordem dos 150 ms, o X.25 proporciona uma ligação fiável sobre meios de transmissão pouco fiáveis e altamente degradados. Dados os seus baixos rendimentos para as redes actuais, e a sua idade (30 anos), está a ser cada vez mais substituído por ligações de tecnologias mais avançadas.



Frame-Relay

O F.R. foi inicialmente proposto em 1984, mas foi em 1990 que foi criado um consórcio com grandes empresas de redes para o seu desenvolvimento e internacionalização. O F.R., ao contrário do X.25, tira partido das vantagens dos meios de transmissão mais recentes, como a fibra óptica. Estes meios de transmissão são muito mais fiáveis que os anteriores pares de cobre ou cabos coaxiais. Os meios de transmissão, sendo mais fiáveis, permitem que se dispense mecanismos de correcção de erros, tornando a transmissão de dados mais eficiente.

O F.R. pode variar a velocidade de ligação entre os 64 Kbps e os 34 Mbps, dependendo do contrato estabelecido com o fornecedor de serviço. Utiliza técnicas de comutação de pacotes, podendo estas ser combinadas com técnicas de comutação de circuitos. O custo destas ligações tende a ser mais barato que linhas privadas de acesso dedicado.

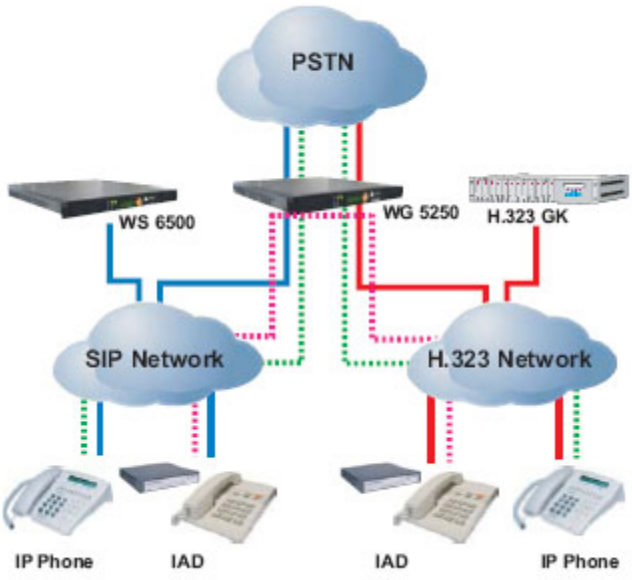


T1/E1

A designação T é utilizada nos Estados Unidos, enquanto que a ligação E é utilizada na Europa. Essencialmente ambos correspondem a um acesso primário RDIS. O acesso primário RDIS corresponde a uma linha, que pode ser em fibra óptica ou cobre, que contém todos os canais digitais possíveis de ter com apenas um cabo. Cada linha T1 tem 24 canais RDIS, enquanto que uma linha E1 tem 30 canais. A sua largura de banda é também proporcional a este número. Uma linha T1 tem um ritmo de transmissão de 1,5 Mbps, enquanto que uma ligação E1 tem 2,048 Mbps, correspondendo a 30x64 kbps por canal.

O seu preço é também proporcional, podendo chegar a custar várias centenas de euros por cada ligação T1 ou E1. Estes cabos podem ainda ser agrupados numa hierarquia:

- DS0 (1 linha digital RDIS) = 64 kbps
- Acesso básico RDIS = 2DS0 + 1D = 144 kbps
- E1 = 30 DS0 = 2,048 Mbps
- E3 = 30 E1 = 64 Mbps
- OC3 = 80 E1 = 160 Mbps
- OC12 = 4 OC3
- OC48 = 4 OC12
- OC192 = 4 OC48 = 10 Gbps

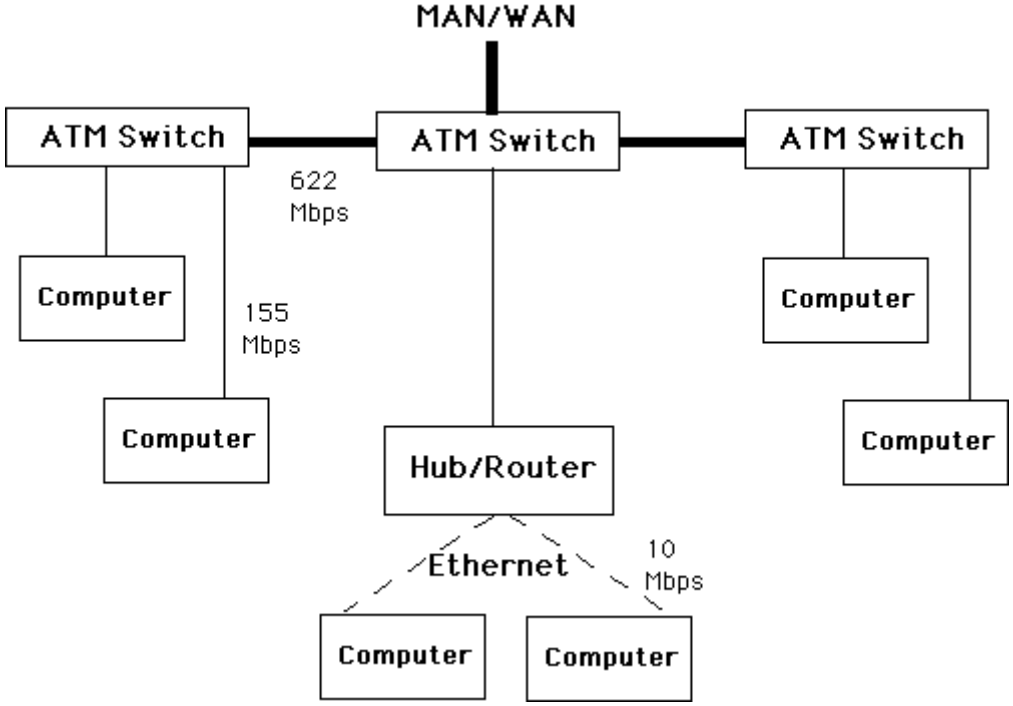


ATM

As redes ATM (Asynchronous Transfer Mode) são cada vez mais utilizadas para ligações centrais nas grandes empresas. Baseiam-se, muito sucintamente, na comutação de células de comprimento de 53 bytes, podendo ser entendida como uma tecnologia de comunicação de dados que congrega vários serviços. Estas células ATM são transmitidas independentemente do meio de transmissão, podendo ser transportadas sobre PDH ou SDH, uma vez que são transparentes para o meio de transmissão. Esta comutação de células de comprimento fixo torna a adaptação de largura de banda a novos serviços extremamente flexível. Estas células de tamanho fixo proporcionam uma transmissão de alta qualidade e baixos tempos de latência, deixando de existir o problema de latência variável quanto maior fosse o tamanho do frame.

A largura de banda das ligações ATM varia de acordo com o tipo de meio de transmissão e com a qualidade se serviço, podendo ir até aos 155 Mbps, sendo ideal para transmissões de *vídeo-on-demand*, *tele-medicina* e *e-learning*.

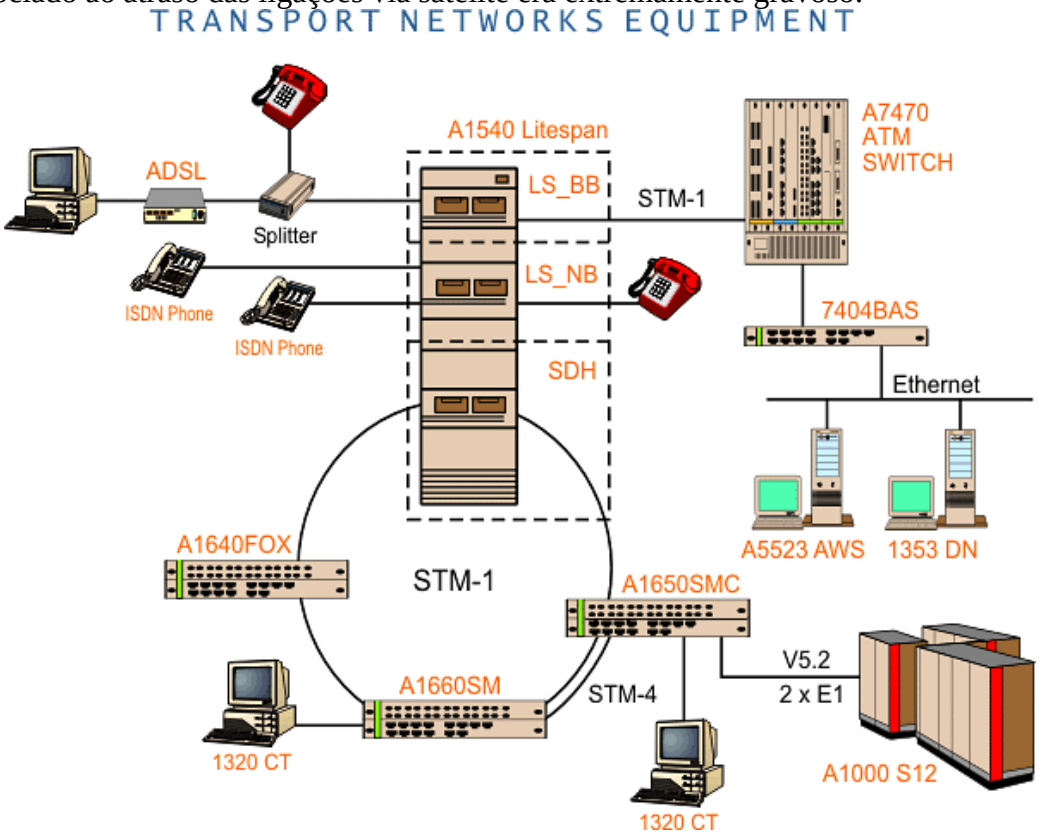
O ATM é também uma tecnologia que permite a integração de vários serviços sobre a mesma estrutura, serviços tais como a voz, o vídeo, dados e multimédia, evitando assim a situação em que existem diferentes redes baseadas em diferentes tecnologias. As redes ATM estão praticamente implementadas em todo o mundo.



SDH

Durante a última década, tem-se verificado uma total renovação dos sistemas de telecomunicações. Com a introdução de novos serviços surgiu a necessidade de se inserirem novas tecnologias nas redes com o intuito de satisfazer a procura de mais largura de banda por parte dos clientes. Um dos casos típicos é a introdução dos sistemas de transmissão da tecnologia SDH (Synchronous Digital Hierarchy) em detrimento da tecnologia PDH (Pleosíncrona). Assim, de forma muito sucinta, esta tecnologia SDH tem como principais inovações a possibilidade de ter débitos mais elevados (logo maior largura de banda) que podem ir até aos 10Gbps (o PDH ia até 565Mbps). A própria estrutura da trama permite aceder directamente a outros débitos sem necessidade de desmultiplexagem até aos 2Mbps, 34Mbps ou 140Mbps e posterior multiplexagem, o que permite valores mais elevados de disponibilidade uma vez que o número de equipamentos na cadeia de transmissão é menor.

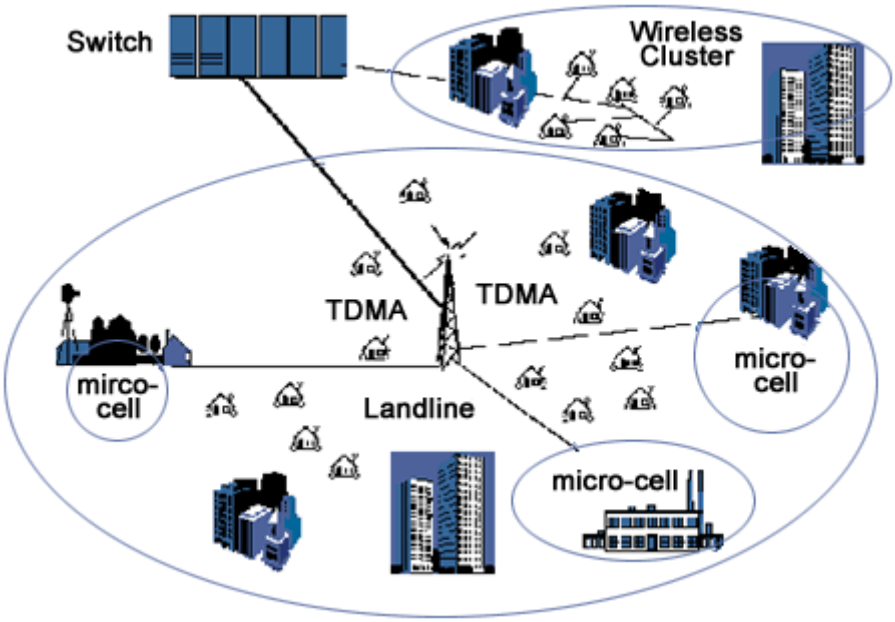
Outra das principais vantagens é que com o SDH passou a haver uma normalização das hierarquias de transmissão, o que não se verificava no PDH, uma vez que havia uma hierarquia japonesa, uma Norte Americana e outra Europeia, que obrigava a adaptadores de débito nas ligações intercontinentais e que no caso do vídeo, associado ao atraso das ligações via satélite era extremamente gravoso.



FWA – Fixed Wireless Access

Esta tecnologia seria a que os novos operadores telefónicos de acesso fixo poderiam adoptar para fazer chegar os seus serviços aos seus clientes. Para a população em geral, esta tecnologia permite acesso à rede nacional de telecomunicações através de pequenas antenas estrategicamente colocadas e com uma área de cobertura muito limitada permitindo que o sinal se propague não através do tradicional par de cobre, ou até F.O, mas sim por meio Hertziano. As principais vantagens do FWA são os custos de instalação mais baixos, uma vez que é menor o recurso a obras públicas e não são necessários cabos de pares simétricos em cobre para praticamente todas as casas. Além disso, permite uma maior celeridade na instalação do serviço, dado que uma única antena permite satisfazer vários clientes e existe uma maior flexibilidade na gestão do equipamento, uma vez que este pode ser novamente atribuído, quando um cliente desistir do serviço.

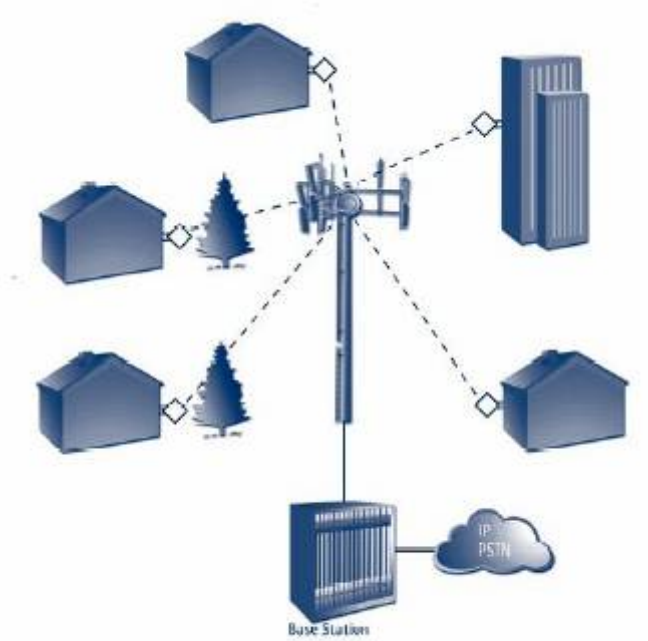
Contudo, o FWA tem uma grande desvantagem, que é a limitação da largura de banda disponível, o que inibirá a prestação de serviços de elevado débito. As estimativas indicam que daqui a 10 anos, a maioria das casas terá acessos de 2 a 34Mbps, o que provavelmente matará esta tecnologia à nascença, uma vez que ela se destina exclusivamente a serviços de telefonia e acesso à Internet nos débitos actuais 56Kbps.



BWA – Broadband Wireless Access

Esta tecnologia encontra-se em fase de laboratório e as previsões apontam para uma utilização de largura de banda na ordem de 1GHz a 40GHz por operador. Nesta tecnologia, o sinal será difundido via difusão e serão utilizadas modulações do tipo QAM que o tornam mais resistente a fenómenos atmosféricos. Apesar do BWA ter vários concorrentes, nomeadamente o xDSL, Cable Modem, Broadband Multimédia Satellite Services ou Power Line Technology, tudo leva a crer que esta irá ser a tecnologia do futuro, no que se refere ao acesso aos clientes residenciais e PMEs, estando previstos débitos de 8 a 34Mbps. Assim, e muito resumidamente, esta tecnologia permite capacidades de transmissão com débitos elevados e também permite uma integração de serviços (porque é de banda larga) e uma melhor gestão dos recursos (porque os serviços vão todos juntos). Para além de todas estas vantagens, a nível tecnológico, o BWA tem custos de instalação muito inferior aos de tecnologia com fios e a sua instalação é muito mais rápida.

A nível de aplicações e serviços que o BWA irá suportar, é de realçar o acesso à Internet de alta velocidade, acesso a LAN remotas, transferência de dados e videoconferência. Numa 2ª fase, estão previstos, entre outros, serviços de vídeo desk-to-desk, tele-medicina, vídeo telefonia, estando também previstos serviços de telefonia para particulares e empresas. Relativamente aos serviços de difusão, temos os canais de TV digitais e TV interactiva com canais de retorno em banda estreita, para serviços tele-shopping e outros.



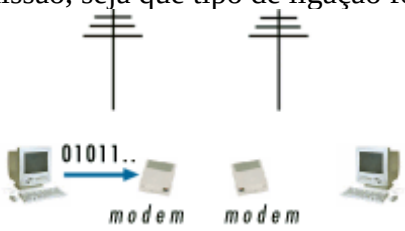
Simplified BWA Network

Dispositivos de Rede

Para colocar uma rede a funcionar, seja ela de que tipo for e que topologia tenha, não basta ligar os cabos entre dois pontos aleatórios. Existe todo um conjunto de máquinas e dispositivos que trabalham para que a rede realmente funcione, e que a transmissão da informação se processe de maneira suave e com o menor número de erros possível.

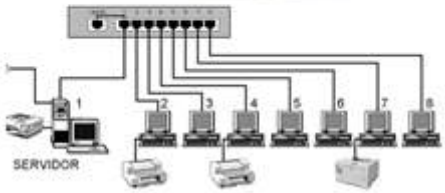
Modem

O modem é um dispositivo que permite a ligação ponto a ponto entre equipamentos terminais. A sua função é converter os dados digitais do computador e adaptá-los ao meio de transmissão, seja que tipo de ligação for.



Placa de Rede

Este tipo de dispositivos garante uma ligação dedicada a tempo inteiro de um equipamento terminal a uma rede. É essencialmente um conversor de acesso ao meio, que transforma os dados dos equipamentos, formatando-os de modo a obedecerem a um determinado protocolo de comunicação de rede (Ethernet, Token-Ring, …). Qualquer equipamento que esteja ligado a uma rede tem um dispositivo deste tipo.



Switch

Este dispositivo de rede efectua uma comutação dos seus circuitos internos de modo a estabelecer uma ligação entre dois equipamentos. Estabelece, por assim dizer, uma ligação directa entre dois dos seus portos para permitir a comunicação entre os terminais.

A grande desvantagem do Switch é que com este dispositivo de rede não é possível efectuar *braodcasts* para a rede, uma vez que as ligações são ponto a ponto.
A utilização de um dispositivo desta natureza numa rede do tipo Ethernet, transforma a sua topologia numa rede em Estrela, sendo o switch o elemento central. Os switch permitem basicamente segmentar redes tal como as bridges, mas com um desempenho muito superior.

Os switch transferem os pacotes entre os diversos segmentos através de uma matriz interna de comutação, em que toda a comutação é feita na sub camada MAC. Quando um pacote chega ao switch, o endereço de destino é analisado e é estabelecida uma ligação ao segmento onde se encontra esse destino. Os pacotes seguintes são encaminhados por essa ligação sem necessidade de os armazenar/enviar como as bridges.

Hub

Este dispositivo interliga vários computadores entre si, à semelhança do switch. A principal diferença entre eles reside no facto de cada pacote transmitido para o hub ser depois transmitido a todos os outros elementos, efectuando-se assim um *broadcast* da informação. Os hubs vão criar, com a sua utilização uma topologia em barramento.
Outra característica dos hubs é a divisão da largura de banda utilizada. Se um hub funciona a, digamos, 100 Mbps, e está ligado a 5 computadores, então cada computador só vai ter uma largura de banda de rede de 100/5=20 Mbps. Este problema não existe com os switch, uma vez que as ligações são ponto a ponto.

A interligação de diversos hubs permite a constituição de configurações mais elaboradas e também mais frequentes, como a topologia em árvore. A interligação destes é feita através de portas de uplink, que trocam os condutores de transmissão-recepção, para que a comunicação seja possível entre dois hubs.

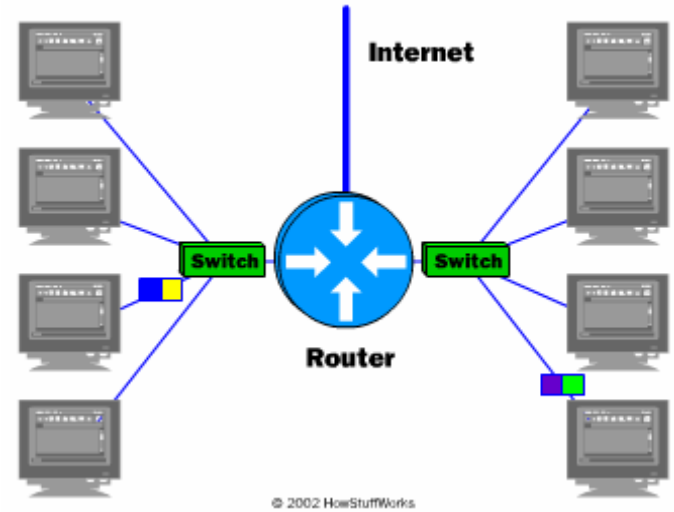
Bridge

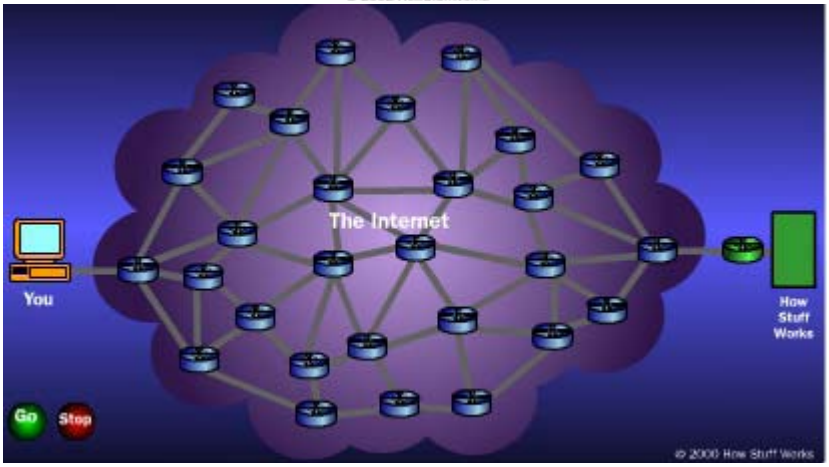
Nas redes de comunicação, este dispositivo interliga duas **redes locais** (LAN) que usam o mesmo protocolo (ex: Ethernet,Token-Ring). Através da análise do bloco de dados, este dispositivo sabe se o destinatário é da rede actual ou da rede vizinha, após o qual o envia para a rede destinada. Essa análise é possível, pois é mantida uma tabela em que o dispositivo regista os utilizadores de cada rede à medida que vai recebendo e enviando blocos de dados. Pode-se considerar que uma bridge é um switch com apenas dois portos.

Router

Este dispositivo pode ser implementado em hardware ou em software. O Router serve para unir vários segmentos de rede, ao contrário da bridge que une apenas dois. Ele determina qual a próxima rede para qual o bloco de dados tem de ser transmitido, com o objectivo de chegar a um determinado destino. O router está ligado, pelo menos, a duas redes e decide o modo como a informação vai ser transmitida, baseando-se, para isso, no estado das redes que está interligado. Nessa operação vai mantendo uma tabela onde regista os caminhos possíveis para o envio da informação e o seu estado actual. Desta maneira, consegue um roteamento dinâmico da informação através de uma variedade de redes diferentes.

Os routers são máquinas bastante inteligentes e robustas, podendo estar a funcionar durante bastante tempo sem terem de ser desligados ou reiniciados. Têm muitas capacidades de fazer balanceamento de carga e possibilitam ligações de salvaguarda, por exemplo, estando ligado à Internet a partir de duas interfaces diferentes, em que uma delas apenas entra em funcionamento se a primeira falhar.





Protocolos

Na língua portuguesa existem uma série de regras, definidas pela gramática portuguesa, que qualquer pessoa que queira falar português deve cumprir, sob pena de não ser entendido durante o seu discurso. Existem também, em qualquer sociedade, um conjunto de regras de comportamento e de convivência em grupo, de modo a que as pessoas que convivem nessa mesma sociedade o possam fazer de maneira aberta e sem desagrados. É o caso do aperto de mão como cumprimento, o circular pela direita num passeio, o conduzir pela esquerda, etc. A este conjunto de normas e regras dá-se o nome genérico de **protocolo**.

O conceito de protocolo é também aplicado às redes de comunicação. Para que dois sistemas que estejam ligados a uma mesma rede consigam comunicar, têm de respeitar o protocolo dessa comunicação. Caso o protocolo seja diferente, terá necessariamente de existir uma conversão entre protocolos, o que se poderá chamar de **tradução**.

As necessidades dos Protocolos

Se não existissem protocolos, cedo nos aperceberíamos disso. Os protocolos e a normalização dão um enorme contributo para a vida social humana, apesar de na maioria das vezes passar despercebida. Geralmente é quando não existe normalização ou protocolo que se dá por falta deles. Como exemplo, quando adquirimos um determinado produto e depois nos apercebemos que é de má qualidade, péssima construção, não serve para o que era proposto, é incompatível com outros produtos que já possuímos ou é perigoso para a saúde e a vida humana.

O facto de existirem protocolos e normalizações leva a que muitas destas características negativas desapareçam, pois todos os produtos que comprarmos terão de ter um nível aceitável de qualidade, ou caso contrário não estariam disponíveis. É nestas medidas e normalizações que entram os organismos normalizadores.

Organismos Normalizadores

Organismos Internacionais

ISO – International Organization for Standardization

ISO é uma rede de institutos internacional, composta por 146 membros, sendo um membro por país, cuja sede se encontra em Genebra na Suiça. A sede tem por função coordenar todas as actividades ligadas às normalizações de todos os membros.

A sua função principal é a de reunir consensos relativamente a soluções que cumpram os requerimentos de empresas e as necessidades alargadas da sociedade.

O nome ISO deriva do grego *isos* que significa igualdade. Desde a sua criação em 1947, na altura com apenas 25 membros, o ISO tem já definidas 13700 normalizações internacionais. Estas normalizações ocupam todos os campos do conhecimento, variando desde a agricultura e a construção, passando pela engenharia mecânica e medicina, até às mais recentes tecnologias de informação e comunicação.

As normas ISO mais conhecidas são, sem dúvida, as normas ISO 9000 e ISO 14000. A primeira providencia os aspectos técnicos para a gestão da qualidade de um produto, a nível dos processos de fabrico e materiais. A segunda, ajuda as organizações a melhorarem a sua produtividade, realizando uma gestão ambiental a todos os níveis.

IEEE – Institute of Electric and Electronic Engineering

O IEEE (lê-se I três És) é uma organização sem fins lucrativos, que conta com mais de 380000 membros individuais em cerca de 150 países. É um organismo ligado a normalizações técnicas e especificações a nível das engenharias electrotécnicas e electrónicas. Através dos seus membros, o IEEE é uma autoridade mundial em áreas tão variadas desde informática, biomedicina e telecomunicações até energia eléctrica, aeroespacial e electrónica de consumo, entre outras.

Através das suas regulares publicações, conferências e regulamentação de normas, o IEEE produz cerca de 30% da literatura mundial em engenharia electrotécnica, informática e tecnologias de controlo, organiza cerca de 300 conferências em todo o mundo, e tem cerca de 900 normas e protocolos activos, com mais 700 em desenvolvimento.

As normas e protocolos do IEEE mais conhecidos são ao nível da informática, e definem protocolos de comunicação série e paralelo, tais como as norma V.32 ou V.90, ou ainda protocolos de acesso ao meio tais como Ethernet e Token-Ring.

ITU – International Telecommunications Union

O ITU é uma agência especializada da responsabilidade das Nações Unidas, originalmente criada em Paris em 1865, na altura denominada de International Telegraph Union. Em 1934 o ITU foi criado para suceder a todas as instituições regulamentadoras das telecomunicações, e em 1947 tornou-se afiliada nas Nações Unidas.

Os objectivos do ITU são o de manter e expandir a cooperação internacional para o melhoramento e uso racional de todos os tipos de telecomunicações; promover o desenvolvimento e operação eficiente das facilidades técnicas, de modo a melhorar os serviços de telecomunicações, aumentar a sua utilidade, e torná-los disponíveis globalmente para o público; e coordenar as acções das várias nações de modo a que atinjam estes objectivos.

O ITU é composto por 189 estados membros e está sedeado em Genebra na Suiça. Encontra-se dividido em três grandes grupos de trabalho:

- ITU-R – para o sector das radiocomunicações
- ITU-T – para a normalização do sector das telecomunicações
- ITU-D – para o desenvolvimento das telecomunicações

ETSI – European Telecommunications Standards Institute

Esta é uma instituição europeia sem fins lucrativos, sedeada no sul de França, cuja principal missão é a de produzir as normas para as telecomunicações que são usadas na Europa e não só.

O ETSI contém 786 membros de 56 países, de dentro e de fora da Europa, e representa administrações, operadores de rede, fabricantes de equipamentos, fornecedores de serviço, corpos de investigação e os utilizadores. Como resultado, as actividades levadas a cabo pelo ETSI estão sempre próximas com as necessidades do mercado de telecomunicações.

O ETSI tem um papel preponderante no desenvolvimento de uma grande gama de normas e protocolos que contribuem para uma melhor padronização das telecomunicações no mundo inteiro. O ETSI é reconhecido oficialmente pela Comissão Europeia. É um dos membros mais importantes do ITU, e as suas actuais preocupações prendem-se mais com o desenvolvimento das normas de UMTS, levadas a cabo pelo grupo 3GPP.

W3C – World Wide Web Consortium

O W3C foi criado em 1994 e tem como objectivo desenvolver e melhorar a WWW de modo a que esta atinja o seu máximo potencial. Desenvolve e normaliza protocolos para que isso aconteça e que proporcione a sua internacionalização e interoperabilidade.

O W3C é composto por cerca de 450 membros em todo o mundo e alcançou prestígio internacional devido às suas contribuições na área da Internet e da World Wide Web.

O W3C foi criado primariamente pelo próprio inventor da WWW, em colaboração com o MIT e o CERN. Em apenas 7 anos de existência, o W3C desenvolveu mais de 50 especificações técnicas para a infra-estrutura da WWW. No entanto, dado que a WWW ainda é jovem, ainda existe muito trabalho para fazer, especialmente numa altura em que existe uma convergência da informática, telecomunicações e multimédia. O desenvolvimento da WWW baseia-se em três princípios, impostos pelo próprio consórcio:

• Interoperabilidade – As especificações para a WWW têm necessariamente de ser compatíveis umas com as outras e permitir que qualquer conjunto de hardware e software possam aceder-lhe.

• Evolução – A WWW deve ser capaz de acomodar novas tecnologias. Os princípios de desenho tais como simplicidade, modularidade e expansibilidade irão permitir que esta evolução se processe de maneira suave.

• Descentralização – sem dúvida o princípio mais difícil de aplicar, uma vez que para que a WWW se torne global, a estrutura onde assenta, ou seja a Internet, deve eliminar dependências de registos centrais. As especificações e protocolos desenvolvidos por este consórcio levaram ao aparecimento e padronização das linguagens de programação para a Web, HTML, XML, entre muitos outros. Na figura seguinte, apresentam-se alguns exemplos dos protocolos criados pelo W3C.

UNICODE Consortium

Numa única frase, o Unicode providencia um código numérico para cada carácter, independentemente da plataforma, independentemente do programa, independentemente do idioma. Por outras palavras, o Unicode é um standard criado para representar qualquer carácter por um código numérico, de modo a que esse código, em qualquer plataforma, dê sempre origem ao mesmo caracter.

O *Unicode Consortium* é uma entidade sem fins lucrativos fundada com o objectivo de desenvolver, estender e promover o uso do Unicode, que especifica uma representação de texto no software, produtos e padrões modernos. Os membros deste consórcio são organizações e instituições mundiais ligadas à indústria informática e sistemas de informação. O consórcio é suportado apenas por quotas dos seus membros.

Organismos Locais

ANACOM – Autoridade Nacional para as Telecomunicações

A ANACOM, previamente chamada de ICP – instituto das comunicações de Portugal, foi criada em 1981 como órgão do sector das comunicações, exercendo a sua acção na tutela do ministro responsável pela área das comunicações.
O ICP, enquanto instituto público com autonomia administrativa e financeira, iniciou a sua actividade em 1989, tendo por finalidade:

- O apoio ao Governo na coordenação, tutela e planeamento do sector das comunicações de uso público,
- A representação do sector,
- A gestão do espectro radioeléctrico.

Prosseguindo as suas atribuições de acordo com uma perspectiva integrada do desenvolvimento das comunicações em Portugal, o ICP actuava em três grandes áreas, agora da responsabilidade da ANACOM:

Assessoria ao Governo, no domínio das medidas de política de comunicações, preparação de legislação e pareceres, representação do Estado Português em organismos internacionais e cooperação internacional;

Regulação do Mercado, no domínio da organização do sector, atribuição e supervisão de licenças e autorizações, estabelecimento de preços, consignação de frequências, controlo da qualidade dos serviços, resolução de conflitos e defesa do consumidor;

Técnica, na gestão do espectro radioeléctrico, fiscalização, certificações e avaliação de conformidade de equipamentos de comunicações

FCCN – Fundação para a Computação Científica Nacional

A FCCN é uma instituição privada sem fins lucrativos designada de utilidade pública que iniciou a sua actividade em Janeiro de 1987. Desde então, com o apoio das Universidades e diversas instituições de I&D nacionais, a FCCN tem contribuído para a expansão da Internet em Portugal.
Como principal actividade a FCCN tem o planeamento, gestão e operação da Rede Ciência, Tecnologia e Sociedade (RCTS), uma rede de alto desempenho para as instituições com maiores requisitos de comunicações, tais como as Universidades e outras instituições governamentais, constituindo-se assim uma plataforma de experimentação para aplicações e serviços avançados de comunicações.

A RCTS é uma rede informática que usa os protocolos da Internet para garantir uma plataforma de comunicação e colaboração entre as instituições do sistema de ensino, ciência, tecnologia e cultura.
Para além da gestão da RCTS, a FCCN é a entidade competente para a gestão do serviço de registo de domínios.pt.

Os Standards

Os organismos descritos anteriormente, juntamente com muitos outros, desenvolvem constantemente protocolos e normas de forma a facilitar as telecomunicações a todos os níveis aos utilizadores.

A nível das telecomunicações são definidas normas e standards que possibilitam essas comunicações, quer em redes móveis, quer em redes fixas. Como exemplo, temos o GSM, o GPRS e o UMTS, normas que foram ou estão a ser desenvolvidas por organismos competentes na área, de modo a torná-las o mais genéricas e úteis possíveis. No que respeita às redes de dados e comunicações de dados, os protocolos Ethernet, Token-Ring, e as normas V.XX, bem como as especificações técnicas das ligações por fibra óptica, cabo coaxial, Frame-Relay, são também elas desenvolvidas e mantidas por entidades regulamentadoras na área.

Numa área mais específica da Internet e da World Wide Web são mantidos, desenvolvidos e regulamentados protocolos de comunicação, que se baseiam num modelo genérico, tais como o HTML, XML, WML, no que respeita ao software, e protocolos como o TCP/IP, HTTP, FTP, POP, ICMP, entre muitos outros no que respeita também ao hardware.

Standards e Protocolos		
Telecomunicações	Redes de Dados	Internet e WWW
GSM	V.XX	HTML
GPRS	DSL	XML
UMTS	Cabo	WML
W-CDMA	F.R.	TCP/IP
TDMA	F.O.	HTTP
FDMA	X.25	FTP
RDIS	Ethernet	TELNET
TV	Token-Ring	ICMP
HDTV	Token-Bus	POP
MPEG	Pinagem de Cabos	SMTP
AM/FM	Desenho de circuitos eléctricos	DNS
PSK/FSK/ASK	Desenho de aplicações informáticas	

Códigos de Representação de Caracteres

Os caracteres utilizados para escrever no computador cumprem, também eles, determinadas normas de modo a obedecer aos protocolos estabelecidos de representação de caracteres. Esses códigos são mantidos e actualizados pelos organismos normalizadores. O ISO define a norma 8859 como a norma que representa todos os caracteres possíveis de representar no mundo inteiro. A partir desta norma desenvolveram-se alfabetos de representação de caracteres.

ASCII

O American Standard Code for Information Interchange é um subgrupo do UNICODE que utiliza 7 bits de representação. Foi mais tarde expandido para 8 bits, de modo a poder suportar caracteres especiais, tais como os acentuados, próprios de cada país. A cada conjunto ASCII é chamada uma página de códigos. Cada computador tem uma página de códigos activa de cada vez, sendo a mais utilizada a número 850, correspondendo aos caracteres latinos internacionais.

O ASCII é o alfabeto mais utilizado no mundo. Todas as marcas de computadores mundiais suportam este alfabeto.

Alfabeto GSM

Também o protocolo GSM utiliza caracteres para a comunicação. Estes são bastante mais utilizados quando enviamos SMS ou quando acedemos à Internet via WAP. O Alfabeto GSM é um subconjunto do UNICODE com 7 bits de representação. Nele se incluem todos os caracteres suportados na comunicação GSM. Mais tarde, com o desenvolvimento dos telemóveis, estes passaram a suportar mais caracteres que o próprio GSM, provocando com que os caracteres não definidos no protocolo nem sempre chegassem ao destino.

Protocolos de Redes

Nos primórdios das redes, todas as funcionalidades das redes de comunicação eram implementadas a nível de hardware. O software tinha como única tarefa a supervisão das funções implementadas, bem como a correcção de alguns outros detalhes da comunicação.

Devido às dificuldades de interligação de dispositivos de origens diferentes, esta metodologia tornou-se difícil de manter e rapidamente obsoleta. A solução estava na delegação integral do controle da comunicação para o software, mais flexível e barato do que o seu antecessor em hardware.

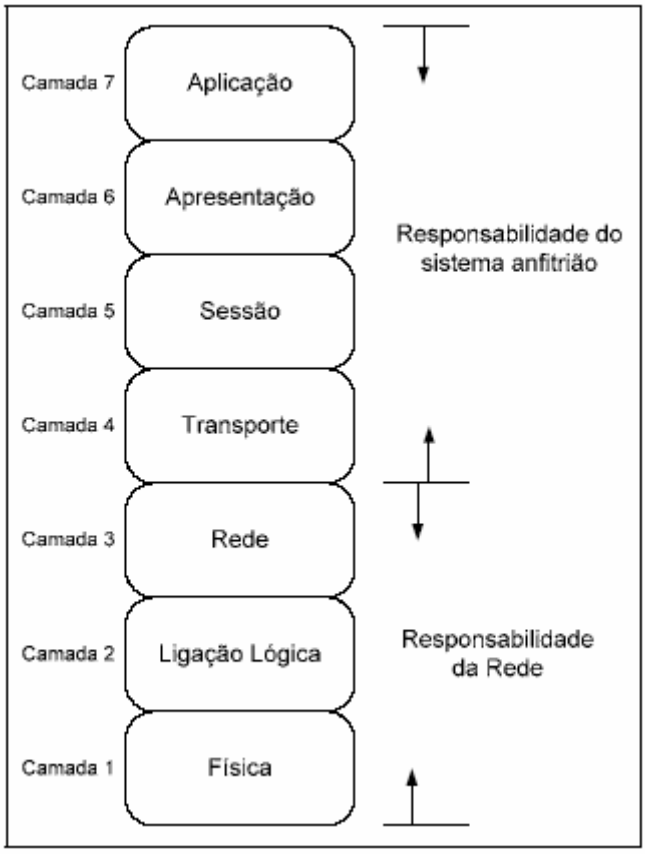
Para reduzir a complexidade do desenvolvimento do software de rede, este foi organizado como um sistema de camadas com funcionalidades distintas. Esta topologia garante que a camada inferior vai proporcionar uma abstracção dos detalhes de implementação da comunicação à camada superior, através da oferta de vários serviços. Paralelamente, o software de rede garantia, ainda, a comunicação entre camadas equivalentes em diferentes sistemas, através dos vários protocolos de rede já existentes. Esses definem acordos entre camadas equivalentes sobre o modo como a comunicação se processa, bem como os recursos utilizados pela mesma.

A transmissão propriamente dita não é assim tão linear. Quando uma camada quiser transmitir informação para outra equivalente noutro sistema, ela passa-a para a camada inferior que a processa. Esta passagem de informação entre camadas contíguas volta a existir até que a informação chegue à última camada (ou primeira, conforme o ponto de vista), que transmite fisicamente a informação recebida sobre um meio físico de transmissão. Do outro lado, a camada equivalente recebe a informação e faz com que a mesma, passe pelo processo inverso até chegar à camada desejada.

Ao conjunto de protocolos utilizados pela rede chamamos de pilha protocolar e, em conjunção com as camadas e respectivos serviços é definida a arquitectura de rede usada.

Modelo OSI

Em 1978 o ISO lançou uma recomendação para um standard de uma arquitectura de rede, que definisse as relações e interacções entre serviços de rede e funções entre os diversos protocolos e interfaces presentes nessa arquitectura. Esta recomendação é hoje largamente aceite sob a forma de uma pilha protocolar de 7 camadas[3] e é conhecida como *Open Systems Interconnection – Reference Model*. A sua forma final foi estabelecida em 1984, com a colaboração de várias empresas de telecomunicações e informática Na altura deveria ser um modelo teórico e prático para as comunicações de dados. Devido ao aparecimento de outros protocolos paralelos, que acabariam por se tornar mais populares, o modelo OSI-RM passou a ser apenas um modelo teórico. Tal como o nome indica, é apenas um **modelo de referência** e não representa nenhuma implementação preferida. Serve apenas como um modelo de trabalho para standards que possam ser aplicados em cada camada por uma variedade de protocolos.



Camadas do Modelo OSI

As **primeiras 3 camadas** (Física, Ligação lógica e Rede) aplicam-se especificamente às arquitecturas das redes locais. Concentram-se na transmissão, construção de tramas[4] e roteamento de pacotes entre máquinas adjacentes. Os protocolos nestes níveis englobam diferentes tecnologias de transmissão, tais como satélite, fibra óptica, cabo coaxial, etc., bem como uma variedade de topologias de rede e diferentes métodos de acesso.

Enquanto que os três níveis inferiores são dependentes da tecnologia, os três níveis superiores são independentes. Quando, no modelo OSI, passamos das camadas inferiores para as superiores, a ênfase passa das funções de hardware e software que asseguram uma transmissão condigna de sinais, para serviços associados a aplicações que correm em computadores ou outros aparelhos.

A **camada de transporte** serve como a fronteira entre as funções de comunicação de dados das camadas inferiores, e as funções de processamento de dados das camadas superiores. Funcionalmente, a camada do meio trabalha com a detecção e correcção de erros, sequenciação de mensagens, endereçamento fim a fim e multiplexagem. Uma função básica desta camada é a subdivisão das mensagens das camadas superiores em pacotes, para serem passadas às camadas inferiores.

Acima da camada de transporte está a **camada de sessão**, que trata das funções lógicas necessárias para efectuar troca de dados de uma forma ordeira. Uma camada de sessão inclui, como mínimo aceitável, um meio de duas entidades de apresentação estabelecerem, usarem e terminarem uma ligação, denominada de **sessão**. A camada de sessão serve como a interface de utilizador para a rede.

Em seguida encontra-se a **camada de apresentação**, que permite que o utilizador disponha de uma variedade de serviços que possam ser úteis para um modo particular de transferência de dados. Exemplos disto são a encriptação e compressão de dados. A **camada de aplicação**, a mais alta das sete no modelo, OSI, trata da formatação dos dados a apresentar ao utilizador. A composição e funções desta camada são altamente dependentes da aplicação de software utilizada.

Camada Física

A transmissão real de bits sobre um suporte físico é da responsabilidade da camada física. Ela tem de garantir que um bit transmitido de um ponto seja igual ao recebido noutro ponto.

A sua definição vai centrar-se nos aspectos físicos, mecânicos e eléctricos do suporte físico usado para a transmissão, bem como nas interfaces utilizadas para proporcionar a transmissão de bits. Vai ainda definir o modo como os bits são representados, quer seja em voltagens por cabos de cobre ou raios de luz via fibras ópticas.

Principais funções da camada física:

- Define Voltagens e impulsos eléctricos
- Especifica cabos, conectores e interfaces de media
- Especifica distâncias máximas de ligação entre estações
- Providencia mecanismos de detecção de colisões para o método de acesso CSMA/CD e seus derivados.

Camada de Ligação Lógica

O propósito básico da camada de ligação lógica é o de estabelecer, manter e libertar ligações lógicas entre nós da rede. Uma ligação lógica pode consistir em um ou mais meios físicos de transmissão, incluindo cabos, fibras ópticas, ligações *wireless* ou canais de satélite.

Os equipamentos localizados nos nós comunicantes podem ser terminais, computadores, equipamentos de comutação ou qualquer outro equipamento que caiba na designação de DCE. A camada de Ligação Lógica controla mecanismos como a notificação de erros, a entrega ordenada de tramas e o controlo do fluxo entre os nós intervenientes. Pode ser dividida em duas sub-camadas: Controlo de Acesso ao Meio, e Controlo de Ligação.

Em resumo, as principais funções da camada de ligação lógica são:

- Transferência fiável de dados por um canal de dados
- Adicionar bits de controlo para indicar inícios e fins de transmissão
- Adicionar algoritmos de correcção e verificação de erros
- Distinguir os dados dos bits de controlo
- Providenciar métodos de acesso às topologias de rede envolvidas

Camada de Rede

A principal função da camada de rede é a de providenciar conectividade e o endereçamento entre dois sistemas finais que podem estar localizados geograficamente em diversos segmentos de rede. Faz com que a camada de transporte, que assenta sobre ela, se abstraia da comunicação fim a fim, de modo a libertá-la da necessidade de conhecer algo sobre as características operacionais dos meios de transmissão envolvidos.

Os protocolos de rede estão preocupados com a transferência de pacotes de informação entre entidades das camadas de transporte. Um pacote é um grupo de bits que inclui os dados e mais alguma informação para o endereçamento.

Quando um pacote atravessa diferentes sistemas, outros problemas podem surgir. Os sistemas podem usar técnicas de endereçamento diferentes, não suportar o tamanho de dados enviados, representá-los de maneiras diferentes, etc. A camada de rede deve, então, resolver estes problemas, permitindo a interligação de redes heterogéneas.

As funções da camada de rede são, então:

- Estabelecer circuitos virtuais (rotas) para a transmissão dos pacotes
- Providenciar serviços de datagrama
- Endereçar equipamento de rede nas rotas dos pacotes
- Dividir as mensagens de transporte em pacotes e juntá-los na recepção
- Controlar a congestão da rede
- Reconhecer prioridades nas mensagens e enviá-las na ordem correcta

Camada de Transporte

A camada de transporte é responsável por estabelecer serviços de transporte de dados entre processos do utilizador, em vez de apenas entre equipamento. É a primeira camada que oferece uma escolha entre protocolos alternativos. Os utilizadores devem assim escolher qual o melhor protocolo que se ajusta às suas necessidades.

O objectivo da camada de transporte é o de fornecer todos os serviços e funções necessários à satisfação da qualidade de serviço requisitada pela camada de sessão. A qualidade de serviço pode ser expressa em parâmetros como a capacidade do canal, a taxa de erros, o tempo de atraso, custo, segurança e prioridade.

As funções da camada de transporte são:

- Estabelecer ligações de transporte de dados fim a fim, de uma maneira fiável
- Multiplexar endereços dos utilizadores finais na rede
- Providenciar detecção de erros e recuperação de dados
- Controlar o fluxo de dados, de modo a prevenir que um sistema sobrecarregue o outro com dados
- Monitorizar a qualidade de serviço
- Separa e Junta as mensagens da sessão

Camada de Sessão

Tal como o nome indica, a camada de sessão estabelece, gere e termina sessões entre aplicações. A camada de sessão lida com funções lógicas que permitam uma transferência de dados de maneira ordeira. Uma sessão consiste num diálogo entre duas ou mais entidades da camada superior, e a camada de sessão sincroniza este diálogo. Este diálogo pode ser um monólogo, caso a comunicação seja unidireccional, e cabe à camada de sessão controlar este parâmetro.

Outra tarefa da camada de sessão consiste em pegar nos dados em bruto da camada de transporte e adicionar serviços orientados ao utilizador.

Algumas funções da camada de sessão incluem:

- Mapear os endereços para nomes
- Estabelecer ligações e terminações
- Transferência de dados
- Controlar os diálogos (quem fala, quando, por quanto tempo)
- Sincronizar tarefas de utilizador
- Invocar encerramentos abruptos e suaves

Camada de Apresentação

Esta camada protocolar vem resolver vários problemas geralmente comuns na transferência de informação, preocupando-se mais com a sintaxe e semântica da informação em vez da sua transferência fiável, que é gerida pelas camadas inferiores.

O exemplo mais comum está nas diferentes representações que a informação pode ter em sistemas diferentes. Para que os sistemas consigam a compatibilidade, a camada de apresentação pega na informação que vai ser transmitida e converte-a para uma estrutura de dados abstracta processável e compreensível por todos os sistemas. Do outro lado, a camada equivalente, após ter recebido essa estrutura de dados abstracta converte-a para o seu próprio formato, após o qual a informação pode ser processada sem problemas.

A camada de apresentação preocupa-se não apenas com o formato e apresentação dos dados do utilizador (ASCII, EBCDIC) mas também com estruturas de dados usadas por programas. Assim, adicionando à actual transformação de dados que pode ocorrer, a camada de apresentação negoceia a sintaxe da transferência de dados para a camada de aplicação.

As principais funções da camada de apresentação são:

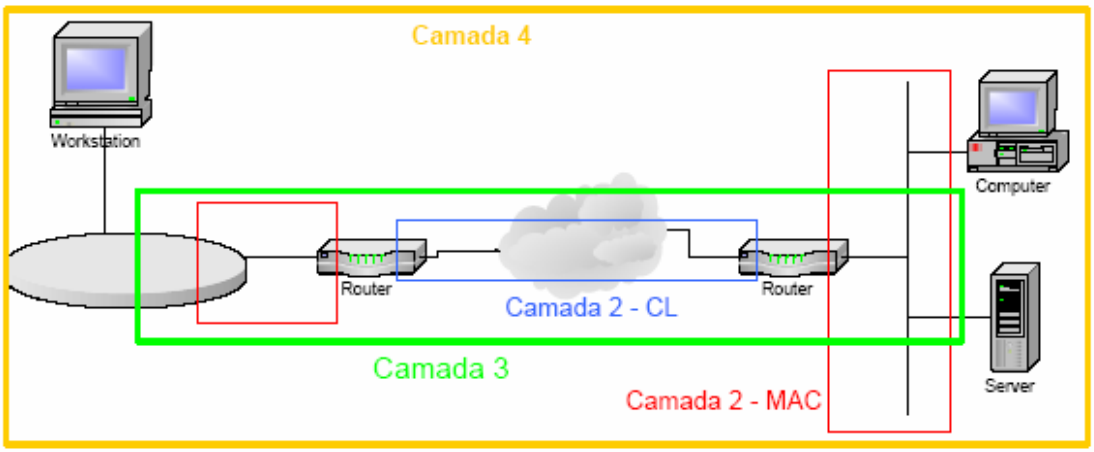
- Estabelecer sintaxes concretas de transferência de dados
- Coordenar a passagem de serviços da camada de sessão para a camada de aplicação

Camada de Aplicação

Esta camada contém os protocolos de aplicação através dos quais o utilizador ganha o acesso à rede. A fronteira entre a camada de apresentação e a camada de aplicação representa a separação dos protocolos impostos pelos arquitectos da rede dos que são seleccionados e implementados pelos seus utilizadores.
A camada de aplicação difere das outras pelo facto de não providenciar serviços às camadas inferiores, mas apenas a processos aplicacionais que residam fora do objectivo do modelo OSI.

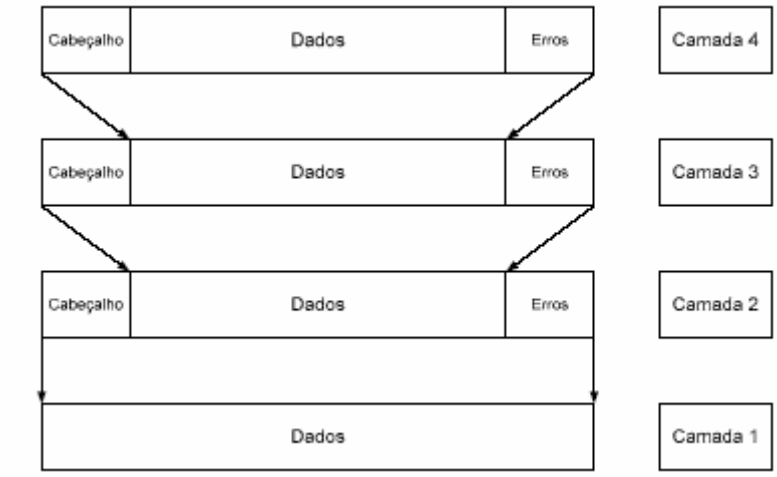
A camada de aplicação identifica e estabelece a disponibilidade dos parceiros interessados na comunicação, sincroniza a cooperação de aplicações e estabelece acordos nos procedimentos de recuperação de erros e controlo da integridade dos dados. Além disso, determina o número de recursos existentes para que a comunicação se processe.
As funções da camada de aplicação são:

- Providenciar serviços de login, verificação de passwords, etc
- Estabelecer acordos na semântica da informação a ser trocada
- Transferência de ficheiros, acesso e gestão de recursos
- Suportar protocolos de software da indústria e comércio, tais como banca, serviços, contabilidade, finanças, entre outros.



Encapsulamento

A camada de aplicação é responsável por interpretar a informação do utilizador e transformá-la de modo a poder ser transmitida. Os Dados gerados por esta aplicação são então transferidos para as camadas inferiores, e posteriormente para o canal de transmissão. Cada camada inferior vai colocar informação extra no início do pacote de dados a transmitir, de modo a poder ser interpretado pela camada equivalente no sistema de destino. Ou seja, vai haver um encapsulamento dos dados em pacotes de informação cada vez maiores, à medida que vamos descendo na pilha protocolar, uma vez que cada camada coloca um cabeçalho e por vezes uns bits de correcção e verificação de erros.



Modelos Práticos

Como referido anteriormente, o modelo OSI é apenas teórico e bastante abstracto, e tenta apenas ser um modelo para que os outros protocolos se possam basear e tornar-se o mais standard possível.
Vários protocolos foram desenvolvidos em paralelo com o modelo OSI e são hoje largamente utilizados, como é o caso do TCP/IP, a Microsoft Networking, o AppleTalk, etc. Na tabela seguinte comparam-se alguns desses protocolos com as camadas do modelo OSI.

<table>
<tr><th>Modelo OSI</th><th>Microsoft Networking</th><th>Novell NetWare</th><th>TCP/IP</th><th>Protocolo ISO</th></tr>
<tr><td>Aplicação</td><td colspan="4">Transferência de Ficheiros, e-mail, Navegação na Web, etc.</td></tr>
<tr><td>Apresentação</td><td>Server Message Block (SMB)</td><td>NetWare Core Protocol (NCP)</td><td rowspan="2">Telnet
FTP
SMTP
Http
TFTP
Etc.</td><td>ISO 8823</td></tr>
<tr><td>Sessão</td><td>Network Basic I/O system (NetBIOS)</td><td>Network Basic I/O System (NetBIOS)</td><td>ISO 8327</td></tr>
<tr><td>Transporte</td><td rowspan="2">Network Basic Extended User Interface (NetBEUI)</td><td>Sequenced Packet Exchange (SPX)</td><td>TCP
UDP</td><td>ISO 8073</td></tr>
<tr><td>Rede</td><td>Internet Packet Exchange (IPX)</td><td>Internet Protocol (IP)</td><td>ISO 8473</td></tr>
<tr><td>Ligação Lógica</td><td colspan="4">Ethernet, Token Ring, FDDI, Frame Relay, X.25, etc</td></tr>
<tr><td>Física</td><td colspan="4">Protocolos da camada física – F.O, Cabo Coaxial, T.P., Wireless, etc.</td></tr>
</table>

Tomando como exemplo os protocolos das telecomunicações móveis, apresentam-se nas figuras seguintes a correspondência entre os protocolos da transmissão de voz no GSM, o protocolo de envio de SMS e o modelo OSI.

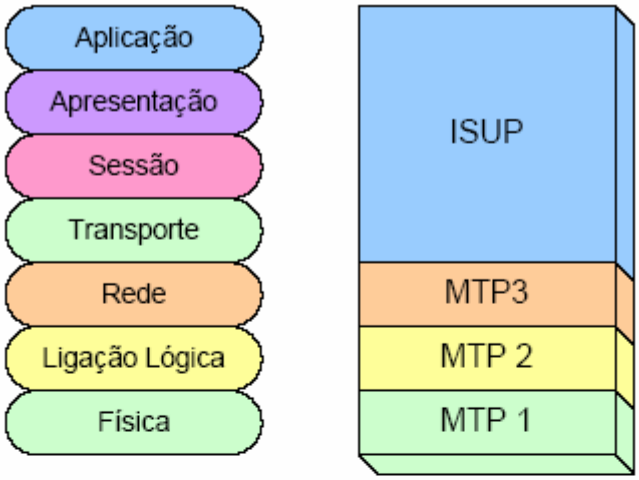
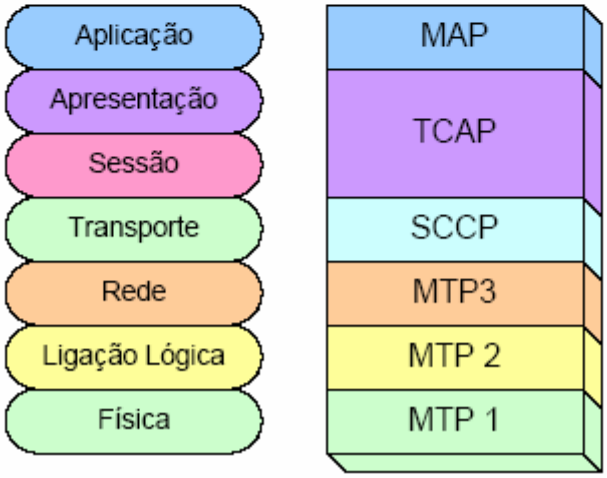


Figura 53 – Protocolo SS7 (GSM) e o modelo OSI



As Camadas inferiores – o Protocolo Ethernet

O protocolo Ethernet, baseado no IEEE 802.3, tem várias especificações. A original era denominada de 10-Base 5, em que o 10 indica o ritmo de transmissão (10Mb/s) e o 5 indica o comprimento máximo dos cabos, coaxiais, em unidades de 100 metros. Novos desenvolvimentos foram feitos até aos dias de hoje (o protocolo Ethernet tem mais de 30 anos) e a especificações mais comuns são o 10-Base T, que opera a 10 Mb/s e o 100-Base TX, que opera a 100 Mb/s. Ambas as especificações utilizam cabos de par entrançado ao invés do tradicional cabo coaxial, e fichas RJ-45, ao invés das fichas BNC que tantos problemas apresentavam a nível mecânico.
As especificações Ethernet cobrem as camadas 1 e 2 do modelo OSI, e as camadas MAC e Física do CSMA/CD. Especificam um barramento com o máximo de 2,5 km de comprimento, ligado em segmentos de 500 metros, uma taxa de transferência de 10 Mb/s ou 100 Mb/s, e um máximo de 1024 estações por barramento.

Em relação à camada física, as funções de um controlador Ethernet (vulgarmente chamado de placa de rede), incluem:

- Codificação de Dados – que inclui a geração e remoção de um preâmbulo para sincronização das tramas, e codificação e descodificação de bits, de modo a traduzir entre formatos de dados
- Acesso ao canal – que inclui a transmissão e recepção de dados codificados em bits, escuta do canal e detecção de colisões. Estas funções são levadas a cabo pelo transceiver presente em qualquer controlador Ethernet

Em relação à camada de ligação lógica, as suas principais funções são:

- Encapsulamento de dados – inclui *framing*, tratamento dos endereços de origem e de destino e detecção de erros no canal físico
- Gestão da ligação – inclui alocação do canal para evitar o mais possível as colisões, e resolução da contenção de colisões.

Trama Ethernet

O formato da trama Ethernet é mostrado na figura seguinte. Cada pacote é uma sequência de bytes, onde o bit menos significativo de cada byte, a começar no preâmbulo, é transmitido primeiro, numa ligação série assíncrona.

Nº Bytes	7	1	6	6	2	46-1500		4
Campo	Preâmbulo	Delimitador de início da trama	Endereço de Destino	Endereço de Origem	Tamanho	Dados	Enchimento	Verificação da trama

As funções dos vários campos da trama são descritas em seguida:

• Preâmbulo – É um padrão de sincronização de 7 bytes composto por zeros e uns alternados, de modo a garantir a sincronização do receptor

• Delimitador de início da trama – Semelhante ao preâmbulo, com apenas 1 byte, mas termina com dois bits a um consecutivos

• Endereço de Destino – Composto por 6 bytes, especifica para que estação o pacote é destinado. O endereço pode ser uma única estação na rede ou pode ser um endereço múltiplo. O primeiro bit indica o tipo de endereço: se 0, trata-se apenas de uma estação; se 1, refere-se a um grupo lógico de estações

• Endereço de Origem – Endereço unívoco na rede que especifica a estação que originou o pacote, em 6 bytes.

• Tamanho – Indica, em 2 bytes, o tamanho dos bytes de dados presentes na trama

• Dados e Enchimento – A especificação IEEE 802 recomenda que o campo de dados tenha um tamanho entre 46 e 1500 bytes. Se os dados fornecidos pela camada de controlo de ligação forem suficientes para perfazer 46 bytes, o mínimo para uma boa operação do protocolo Ethernet, então um número inteiro de bytes de enchimento serão incluídos nos dados até perfazer o tamanho de 46.

• Verificação da trama – Contém 4 bytes usados para o CRC para detecção e correcção de erros. O CRC cobre o endereço de destino, o endereço de origem, o tamanho, os dados e o enchimento.

Endereços de acesso ao meio

No que respeita aos endereços, eles são especificados pela forma XX-XX-XX-XX-XX-XXXX.

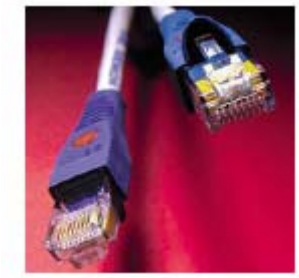
Os endereços de cada controlador Ethernet devem ser únicos na mesma rede. Estes são visíveis ao executar o comando **ipconfig** na linha de comandos do Windows. Para os outros protocolos de rede, também os controladores têm um endereço geralmente de 6 bytes, que é chamado de endereço de acesso ao meio, ou *MAC address*. Um modem, quando ligado a um ISP para o serviço de Internet, possui também um endereço de acesso ao meio. Qualquer protocolo que necessite de identificar o controlador na camada 2 fá-lo através de um endereço deste tipo.

```
        Nome do sistema anfitrião. . . . .: Goliver
        Sufixo DNS principal. . . . . . . :
        Tipo de nó. . . . . . . . . . . . : Híbrido
        Rota IP activado. . . . . . . . . : Não
        WINS Proxy activado . . . . . . . : Não

Adaptador ethernet Ligação de área local:

        Sufixo DNS específico da ligação. :
        Descrição . .  : Realtek RTL8139/810x Family Fast Ethernet NIC
        Endereço físico . . . . . . . . . : 00-08-0D-11-AE-0B
        DHCP activado . . . . . . . . . . : Sim
        Autoconfiguração activada . . . . : Sim
        Endereço IP . . . . . . . . . . . : 192.9.100.6
        Máscara de sub-rede . . . . . . . : 255.255.255.0
        Gateway predefinido . . . . . . . : 192.9.100.1
        Servidor DHCP . . . . . . . . . . : 192.9.100.1
        Servidores DNS. . . . . . . . . . : 193.126.4.34
                                            193.126.4.33
        Concessão obtida.. . : sábado, 21 de Junho de 2005 9:14:18
        Concessão obtida válida até: terça-feira, 24 de Junho de 2005
9:14:18
```

Estes endereços são usados pelas *bridges* e pelos *switches* para estebelecer as ligações entre elementos da rede e para o roteamento de pacotes. Ao receberem um pacote de dados, vão descascá-lo até ao cabeçalho do pacote Ethernet, de modo a determinar o endereço MAC do elemento de destino e assim poderem estabelecer a ligação ao elemento de origem. Podemos assim dizer que tanto a *bridge* como o *switch* trabalham na camada 2 do modelo OSI.

Cabos Ethernet

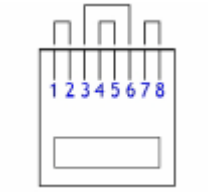
Os cabos Ethernet sofreram várias evoluções na sua especificação. No início eram utilizados os cabos coaxiais, mas o facto da resistência mecânica das fichas não ser a melhor levou a que se passasse a utilizar o cabo de pares entrançados. A última versão do standard que define os cabos Ethernet (EIA 568) recomenda a utilização de cabos de categoria 5 (UTP ou STP) e fichas do tipo RJ-45. Esta configuração permite ligações a 100 Mbps, sendo utilizado nos protocolos 100-Base TX e FDDI.



A recomendação do IEEE é que se respeite a posição dos cabos nas posições certas de modo a evitar a interferência de sinais de um par entrançado para outro. A ligação **directa** deve ser:

- Pinos 1 e 2 são o mesmo par entrançado para transmissão (laranja)
- Pinos 3 e 6 são o mesmo par entrançado para recepção (verde)
- Pinos 4 e 5 são o mesmo par entrançado para bidireccionalidade (azul)
- Pinos 7 e 8 são o mesmo par entrançado para bidireccionalidade (castanho)

Os pinos contam-se da esquerda para a direita, com a tranca da ficha virada para baixo e os contactos para a frente.



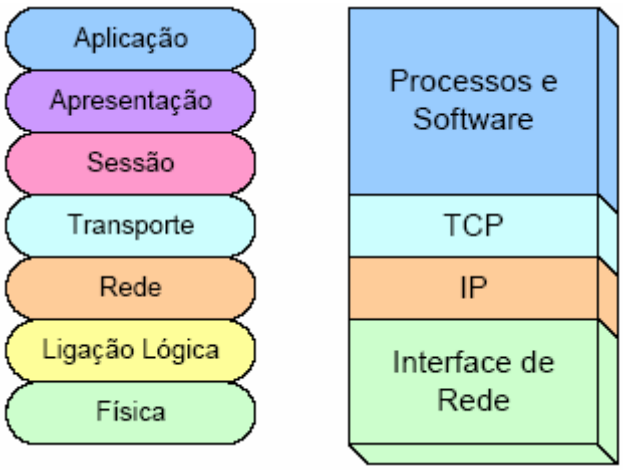
Transmission Control Protocol / Internet Protocol

Os protocolos TCP/IP são uma pilha protocolar para as camadas 3 e 4 do modelo OSI e suporte das camadas seguintes. Pelas descrições anteriores, sabemos que:

• A camada 3 do modelo OSI fornece conectividade fim a fim entre elementos de rede

• A camada 4 do modelo OSI fornece conectividade fim a fim entre aplicações de comunicação

• As camadas 5,6 e 7 são na sua maioria aplicações de comunicação e os seus derivados



Origem

Em meados dos anos 70, o *Defense Advanced Research Projects Agency* publicou uma suite de protocolos para as comunicações entre instituições de pesquisa e desenvolvimento dos Estados Unidos. Quando mais algumas instituições governamentais aplicaram estes protocolos às suas redes, foi fundado um grupo de pesquisa para a sua normalização destes protocolos de comunicação.

O resultado deste desenvolvimento, terminado em finais dos anos 70, deu origem à suite de Protocolos da Internet, dos quais o TCP e o IP são de longe os mais conhecidos. Estes protocolos da Internet podem ser usados para comunicar entre qualquer conjunto de redes interligadas. São também aplicáveis para redes de área local e a redes de área alargada. Nas redes de área local é vulgar utilizar o TCP/IP sobre uma rede Ethernet (camadas 1 e 2).

Protocolos do TCP/IP

O TCP/IP representa não apenas os protocolos IP da camada 3 e o protocolo TCP da camada 4, mas todo um conjunto de outros protocolos que trabalham nas restantes camadas superiores. As camadas 1 e 2 podem trabalhar com qualquer outro protocolo, sendo o mais vulgar, em redes de área local, o protocolo Ethernet.
De forma muito sucinta, podemos dizer que:

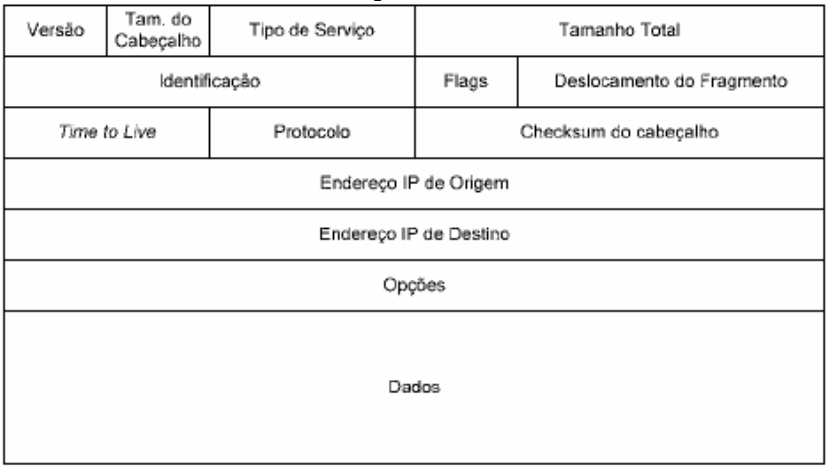
- Os protocolos da camada 3
  - IP – conectividade fim a fim entre elementos da rede
  - ICMP – Testes de conexão fim a fim
- Os protocolos da camada 4
  - TCP – Conectividade fim a fim fiável, com controlo de erros
  - UDP – Conectividade fim a fim não fiável, sem controlo de erros
- As camadas superiores (5, 6 e 7), incluem cerca de 400 protocolos diferentes para as várias aplicações, entre os quais
  - Telnet – Emulação de Terminal
  - FTP – Transferência de ficheiros fiável
  - TFTP – Transferência de ficheiros não fiável
  - SNMP – Gestão dos recursos da rede
  - HTTP – Transferência de Hypertexto
  - SMTP – Transferência de e-mail
  - DNS – Tradução de domínios
  - HTTPS – Protocolo HTTP sobre ligações seguras TSL/SSL
  - RLOGIN – Login remoto
  - NFS – *Network File System*
  - NetBIOS – *Network Basic I/O System*

Internet Protocol – IP

O IP é a camada de roteamento da suite TCP/IP. Pertence, por isso, à camada 3 providenciando conexões fim a fim entre elementos da rede. As suas principais funções incluem a definição do método de endereçamento e a definição dos métodos de roteamento, de modo a enviar os pacotes de dados entre as estações.

Todos os protocolos do TCP/IP à excepção dos protocolos ARP e RARP, usam o IP para rotear as tramas de elemento a elemento. O cabeçalho da trama IP contém informação necessária ao roteamento e informação de controlo associada à entrega do datagrama.

O IP é um protocolo que se baseia nas políticas de melhor esforço e de não conexão, ou seja, no caso da entrega de um pacote conter erros, o nó de destino ou qualquer elemento de roteamento no meio, descarta o pacote e notifica o nó de origem por ICMP que o pacote foi descartado. No caso da política de não conexão, esta diz que não há nenhuma conexão estabelecida entre a origem e o destino. Cada trama pode chegar por caminhos diferentes e em tempos diferentes.



O conteúdo da trama será explicado em seguida:

• Versão – Indica a versão de IP que está a ser utilizada. A última versão oficial é o IPv4, que contém endereços de 32 bits, mas já é usado nalgumas situações o IPv6 que contém endereços de 128 bits.

• Tamanho do Cabeçalho – Indica o tamanho do cabeçalho da trama.

• Tipo de serviço – Especifica de que maneira o protocolo da camada superior lida com a trama. As tramas podem receber prioridades e importâncias neste campo.

• Tamanho total – Especifica, em bytes, o tamanho total da trama, incluindo o cabeçalho e os dados.

• Identificação – Contém um número inteiro que identifica a trama. Este número ajuda a juntar os dados separados pelas várias tramas.

• *Flags* – Campo de 3 bits, dos quais os dois menos significativos controlam a fragmentação. Um especifica se o pacote pode ser fragmentado, o outro indica se o pacote é o último fragmento de uma série de pacotes.

• Time to live – Medido em *hops*, mantém um contador que gradualmente vai ser decrementado até zero, valor no qual o pacote é descartado. Este mecanismo evita que o pacote circule indefinidamente na rede.

• Protocolo – Indica que protocolo da camada superior recebe o pacote após a recepção e tratamento pela camada IP.

• *Checksum* do cabeçalho – Ajuda a verificar a integridade do pacote IP.

• Endereço de Origem – Especifica o nó de origem.

• Endereço de Destino – Especifica o nó de destino.

• Opções – Permite ao IP suportar várias opções tais como segurança e compressão.

• Dados – Contém a informação recebida das camadas superiores.

ARP – Address Resolution Protocol

O protocolo ARP é o responsável pela tradução entre endereços MAC e endereços IP, funcionando assim como a interface entre as camadas 2 e 3 da pilha protocolar TCP/IP. Apenas funciona sobre protocolos de rede local como o Ethernet e o Token-Ring.

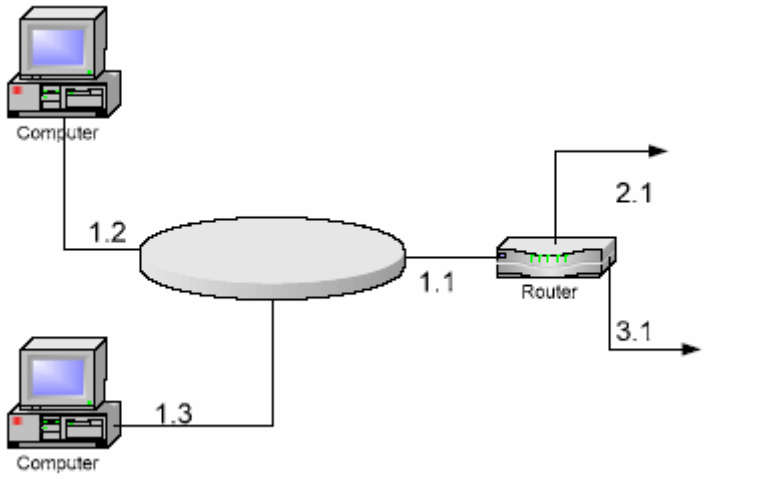
Sempre que é solicitado o seu serviço, o protocolo ARP funciona por tentativas. No caso da transmissão de uma trama para um determinado endereço de destino, um *broadcast* é enviado contendo os endereços IP da origem e do destino, e o endereço MAC da origem. Se a estação de destino estiver viva, uma resposta é enviada de volta com o endereço MAC do destino e o endereço IP. Nessa altura, a estação de origem guarda numa memória temporária (*cache*) os resultados que vai obtendo através da utilização do protocolo ARP. Sempre que é necessário enviar um pacote, é verificado primeiro se o endereço MAC já está na memória, e em caso afirmativo, o pacote é enviado directamente. Esta memória é mantida durante um tempo variável, findo o qual todo o processo necessita de ser recomeçado.

```
Interface: 192.9.100.6 --- 0x2
  Endereço Internet      Endereço físico      Tipo
  192.9.100.1           00-a0-c5-20-51-45     dinâmico
  192.9.100.4           00-04-76-a4-31-db     dinâmico
  192.9.100.5           00-10-a7-03-0b-a1     dinâmico
```

Endereçamento IP

Um dos propósitos da pilha protocolar TCP/IP é disponibilizar um esquema de endereçamento, de modo a proporcionar conectividade entre nós da rede. Este propósito é conseguido pelo protocolo IP, que especifica um método único de endereçamento, conhecido por endereço de Internet.

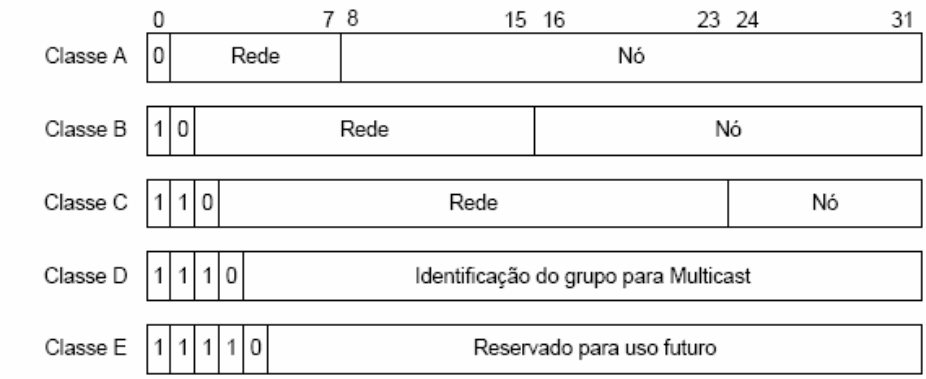
Um endereço IP tem de especificar não só qual o nó correspondente, mas também a que parte da rede pertence o nó. São estas duas partes que compõem o endereço IP: Rede e Nó. O roteamento dos pacotes IP é feito com base nestes dois campo. Em primeiro lugar, o pacote é enviado para a **rede** de destino, e em seguida, dentro dessa rede, é enviado para o **nó** correspondente.



Os 32 bits dos endereços IP são divididos em 4 bytes, separados por um ponto, em que pelo menos um byte identifica a rede (o mais significativo), e os restantes identificam o nó, sendo também no mínimo um byte para esta identificação. São assim possíveis 2_{32} endereços.

Os endereços IP incluem sempre dois campos na sua construção: o endereço IP propriamente dito, que será um identificador único do elemento da rede; e a máscara de rede que indica que parte do endereço IP identifica a rede, e que parte identifica o nó. O número de bytes que identifica a rede é variável, de acordo com a dimensão da rede. Uma grande empresa como a IBM necessita de uma rede com milhares de nós, enquanto que uma rede de uma pequena empresa apenas necessita de algumas dezenas.

De acordo com este critério, os endereços IP são divididos em 5 classes, das quais três para uso geral, e as outras duas para propósitos genéricos. A classe indica, a partir do início do primeiro byte, qual é a máscara usada por omissão.



Os endereços são então da forma que se segue:

- Para a classe A: (1-127).0.0.0 - (1-127).255.255.255
- Para a classe B: (128-191).0.0.0 – (128-191).255.255.255
- Para a classe C: (192-223).0.0.0 – (192-223).255.255.255
- Para a classe D: (224-239).0.0.0 – (224-239).255.255.255
- Para a classe E: (240-247).0.0.0 – (240-247).255.255.255

Como norma, a classe A usa um byte para a identificação da rede, e 3 bytes (24 bits) para a identificação do nó. A classe B utiliza 2 bytes para cada campo, ao passo que a classe C utiliza 3 bytes para a rede e 1 para o nó.

Na prática qualquer endereço IP pode ser utilizado numa rede local, não tendo obrigatoriamente de cumprir as regras da definição de classes. Quando são utilizados endereços IP que não pertencem a nenhuma classe específica, estes são chamados de *classless*.

Existem também alguns endereços IP que estão reservados para usos predefinidos:

- 0.0.0.0 – Define a rede de omissão, e é usado tipicamente em roteamento
- 127.0.0.1 – Endereço de *loopback*. Serve para o nó enviar mensagens para ele próprio, com o objectivo de testar a rede.
- 255.255.255.255 – Os endereços terminados em 255 indicam um *broadcast* e não podem ser usados para identificar nós individuais.

Do mesmo modo, as máscaras de rede são também associadas à classe do endereço IP:

- Classe A: 255.0.0.0
- Classe B: 255.255.0.0
- Classe C: 255.255.255.0

Segmentação de Redes

Quando uma rede tem necessidade de crescer, o seu tamanho e o número de elementos conectados pode tornar impraticável a sua manutenção. Neste caso, o melhor que há a fazer é dividir a rede em segmentos mais pequenos, todos ligados entre si por um router ou um switch. A este processo de divisão de uma rede em segmentos mais pequenos dá-se o nome de **segmentação**.

A segmentação pode e deve ser feita na camada de rede, ao nível dos endereços IP dos elementos. Por exemplo, se queremos uma rede ligada à Internet e o ISP apenas nos forneceu um endereço IP de classe C, podemos dividir a rede em sub-redes mais pequenas, e ligar os vários segmentos através de um router.

Um exemplo prático: se a rede for de classe C poderemos ter 254 elementos conectados com aquela mesma classe. Se utilizarmos 2 bits do campo de elementos para criar uma máscara, estaremos a dividir a rede em 2_2=4 sub-redes.

192	168	1	0-255
255	255	255	0
			00000000

Endereço Original

192	168	1	0-255
255	255	255	192
			11000000

Endereço Modificado

Os quatro grupos de endereços ficarão como:

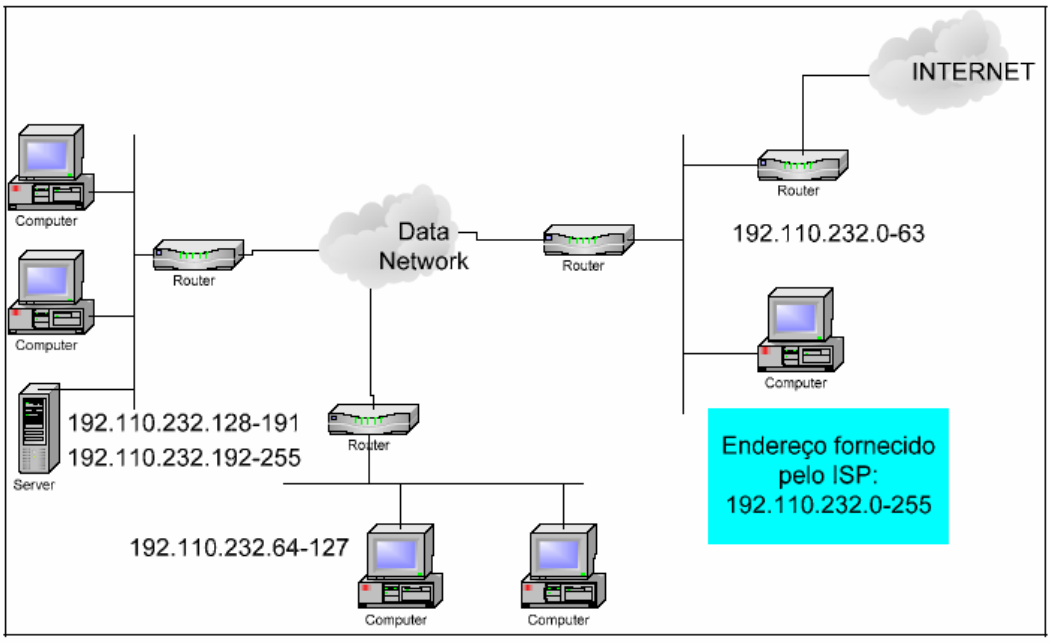
- De 192.168.1.0 a 192.168.1.63
- De 192.168.1.64 a 192.168.1.127
- De 192.168.1.128 a 192.168.1.191
- De 192.168.1.192 a 192.168.1.255

Todos os endereços com máscara de rede **255.255.255.192**.

A segmentação pode ser feita de várias maneiras, dependendo das necessidades de utilização da rede. No entanto, de modo a que a segmentação seja o mais eficiente possível, devem ser cumpridas algumas regras.

O número de identificadores de rede diferentes será determinado pela soma das subredes e das ligações de área alargada, incluindo Internet. O número de identificadores de estações por sub-rede será a soma do número de interfaces TCP/IP presentes, sendo que cada router pode ter mais do que uma interface.

Em seguida, deve-se definir uma máscara de sub-rede de acordo com os requerimentos anteriores. Cada segmento físico da rede deve ter um identificador de rede diferente, de modo a haver uma separação física. Dentro de cada sub-rede, devem ser definidos os endereços IP relevantes e unívocos.



Registo de Endereços IP

Para conectar a uma rede global como é o caso da Internet, é necessário ter um IP válido que cumpra os requisitos das classes pré-definidas. Para um uso privado, tal não é necessário, podendo utilizar qualquer IP, seja ele de que classe for ou mesmo sem classe. É necessário ter o devido cuidado quando é necessário ligar à Internet, de modo a que os endereços IP da rede privada não entrem em conflito com os endereços públicos já existentes.

Deste modo, estão definidos pelo standard determinadas gamas de endereços IP que são garantidas que não existem na rede pública. Como tal, é esta gama de endereços IP que é recomendável utilizar em redes privadas:

- 10.X.X.X de classe A
- 172.16-31.X.X de classe B
- 192.168.X.X de classe C

IPv6

O IPv6 é uma extensão ao protocolo IP, devido a este último se estar a tornar limitativo no número de redes que se podem ainda acrescentar à Internet. Por outras palavras, os endereços de 32 bits disponíveis para a rede pública já são escassos. Assim foi levado a um desenvolvimento do qual surgiu o IPv6, que muito provavelmente será o protocolo utilizado nas redes móveis de 3ª geração, de modo a endereçar os milhões de equipamentos possíveis.

As principais diferenças para o IPv4 residem no aumento do espaço de endereçamento para 128 bits, contra os 32 bits do IPv4, o que implica um aumento significativo do número de endereços públicos possíveis. Outra grande diferença reside nos endereços de *anycast*, o qual é usado para identificar grupos de elementos, no qual um pacote enviado para esse grupo é entregue a apenas um elemento. O formato da trama do IPv6 é também diferente, baseando-se num cabeçalho mais simplificado, mas considerado mais útil.

O IPv6 adiciona também capacidades de Qualidade de Serviço e capacidades de autenticação e privacidade.

Ferramentas do IP

Existem, em qualquer computador ou elemento de rede que trabalhe com o IP, algumas ferramentas úteis para testar os protocolos da camada de rede desta pilha protocolar. São elas o PING e o TRACEROUTE as mais importantes.

O PING é uma ferramenta que utiliza o protocolo ICMP – *Internet Connection Manager Protocol* para testar conectividade entre elementos. Envia um pacote com uma dimensão predefinida até ao elemento com o IP especificado, e espera por um pacote de resposta do destinatário. Se esse pacote for recebido, então existe conectividade entre os dois elementos.

```
A enviar para 195.245.178.1 com 32 bytes de dados:

Resposta de 195.245.178.1: bytes=32 tempo=114ms TTL=252
Resposta de 195.245.178.1: bytes=32 tempo=72ms TTL=252
Resposta de 195.245.178.1: bytes=32 tempo=90ms TTL=252
Resposta de 195.245.178.1: bytes=32 tempo=113ms TTL=252

Estatísticas de ping para 195.245.178.1:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (perda: 0%),
Tempo aproximado de ida e volta em milissegundos:
    Mínimo = 72ms, Máximo = 114ms, Média = 97ms
```

```
A enviar para sapo.pt [194.65.79.190] com 32 bytes de dados:

O pedido excedeu o tempo.
O pedido excedeu o tempo.
O pedido excedeu o tempo.
O pedido excedeu o tempo.

Estatísticas de ping para 194.65.79.190:
    Pacotes: Enviados = 4, Recebidos = 0, Perdidos = 4 (perda: 100%),
```

Quando o PING não recebe resposta do destinatário é porque a ligação não está em condições. Nesse caso, pode-se utilizar o comando TRACEROUTE ou TRACERT para tentar identificar onde é que falha a ligação. O TRACEROUTE vai trabalhar também com o ICMP enviando pacotes até ao endereço de destino, mas vai receber resposta de todos os elementos de rede que se encontrem no caminho, permitindo assim traçar uma rota por onde passa o pacote de dados.

```
A rastrear a rota para dns.net4b.pt [195.245.178.1]
até um máximo de 30 saltos:

  1    62 ms    52 ms    81 ms  213.58.190.129
  2    83 ms    86 ms    75 ms  PLG-02 [195.245.187.180]
  3    79 ms    93 ms    65 ms  SP01-02 [195.245.137.58]
  4   100 ms    93 ms    82 ms  dns.net4b.pt [195.245.178.1]

Rastreio concluído.
```

Os três valores representados em cada linha do comando indicam os tempos médios de transmissão dos pacotes ICMP enviados, à semelhança dos tempos mostrados no comando PING. Quando em vez de um valor numérico obtemos um asterisco (*), então na maior parte dos casos descobrimos a falha onde os pacotes são perdidos, apesar de nem sempre ser verdade. Outras razões incluem o facto do elemento de rede não responder a pedidos de ICMP por questões de segurança, ou o tempo de espera do pacote já ser demasiado longo.

```
A rastrear a rota para sapo.pt [194.65.79.190]
até um máximo de 30 saltos:

  1    74 ms    86 ms    52 ms  213.58.190.129
  2   100 ms    75 ms   280 ms  PLG-02 [195.245.187.180]
  3   115 ms    61 ms    63 ms  GR-02 [195.245.137.93]
  4    91 ms    59 ms   273 ms  195.245.137.87
  5   382 ms    58 ms    61 ms  213.13.138.145
  6    74 ms    70 ms    52 ms  lcatrt2.telepac.net [213.13.135.129]
  7    90 ms    88 ms    66 ms  katrt7.telepac.net [213.13.135.62]
  8     *        *        *     O pedido excedeu o tempo.
  9     *        *        *     O pedido excedeu o tempo.
 10     *        *        *     O pedido excedeu o tempo.
 11     *        *        *     O pedido excedeu o tempo.
```

O TRACEROUTE percorre no máximo 30 elementos (hops) para determinar a rota.

Protocolos da camada 4 – TCP

TCP – Transmission Control Protocol

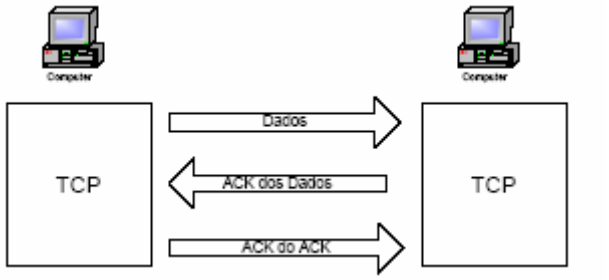
O protocolo TCP providencia ligações fiáveis Full-Duplex e orientadas à conexão para os protocolos que se encontram nas camadas superiores. Transfere os dados de um modo contínuo, onde os bytes são identificados por números sequenciais. O TCP suporta numerosas conversações simultâneas dos protocolos das camadas superiores.

O termo fiável refere-se ao facto do protocolo conter algoritmos que verificam a integridade dos dados recebidos. Após a recepção de um grupo de pacotes é enviado ao emissor um sinal de *acknowledge*, indicando que a transmissão foi bem sucedida. O tamanho do grupo de pacotes é adaptável à performance da rede.

O mecanismo de conexão do TCP funciona da seguinte forma:

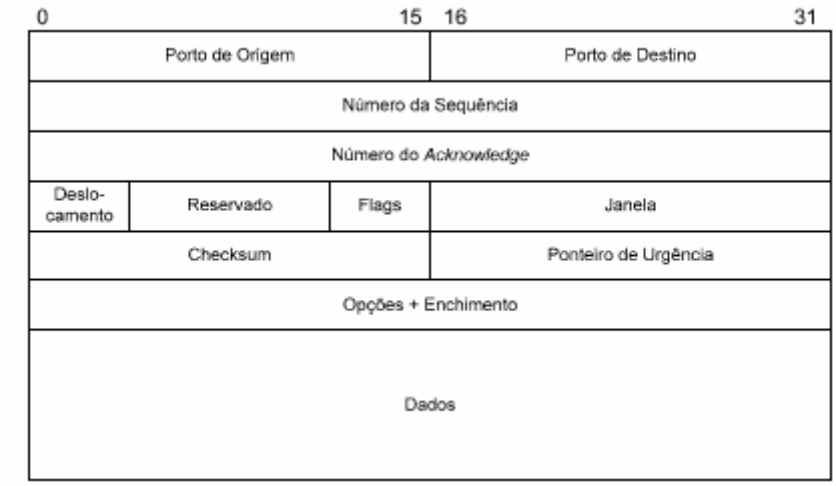
- O remetente envia um pedido de transmissão de dados para o destinatário
- O destinatário aprova a chegada das tramas
- O remetente envia uma trama de Início de Transmissão
- Quando a conexão é estabelecida, o remetente transmite os pacotes de dados através do canal.

De modo a garantir a fiabilidade dos dados transmitidos é utilizado um sistema de *handshake* de três-vias, em que o destinatário envia um sinal de *acknowledge* ao remetente e o remetente responde com um *acknowledge* ao *acknowledge* do destinatário.



Trama TCP

A trama TCP tem o seguinte aspecto:



Como se pode observar, a trama não inclui informação de endereçamento, uma vez que essa responsabilidade é da camada 3 e não do TCP. Contém outros campos igualmente importantes:

• Porto de Origem e de Destino – Identificam os pontos onde os quais os processos das camadas superiores vão receber a informação do TCP. Um porto não é mais que um endereço de software que se destina a identificar pontos de acesso, à semelhança com o número da porta numa rua.

• Número da Sequência – Usado para identificar o número de sequência da trama.

Corresponde ao número do primeiro byte de dados contido na trama.

• Número de *Acknowledge* – Contém o número de sequência do próximo byte de dados que o remetente espera de resposta. Corresponde ao último *acknowledge* que o remetente recebeu.

• Deslocamento – Serve para indicar onde começam os dados, especificando o tamanho do cabeçalho

• Reservado – par uso futuro e expansões do protocolo

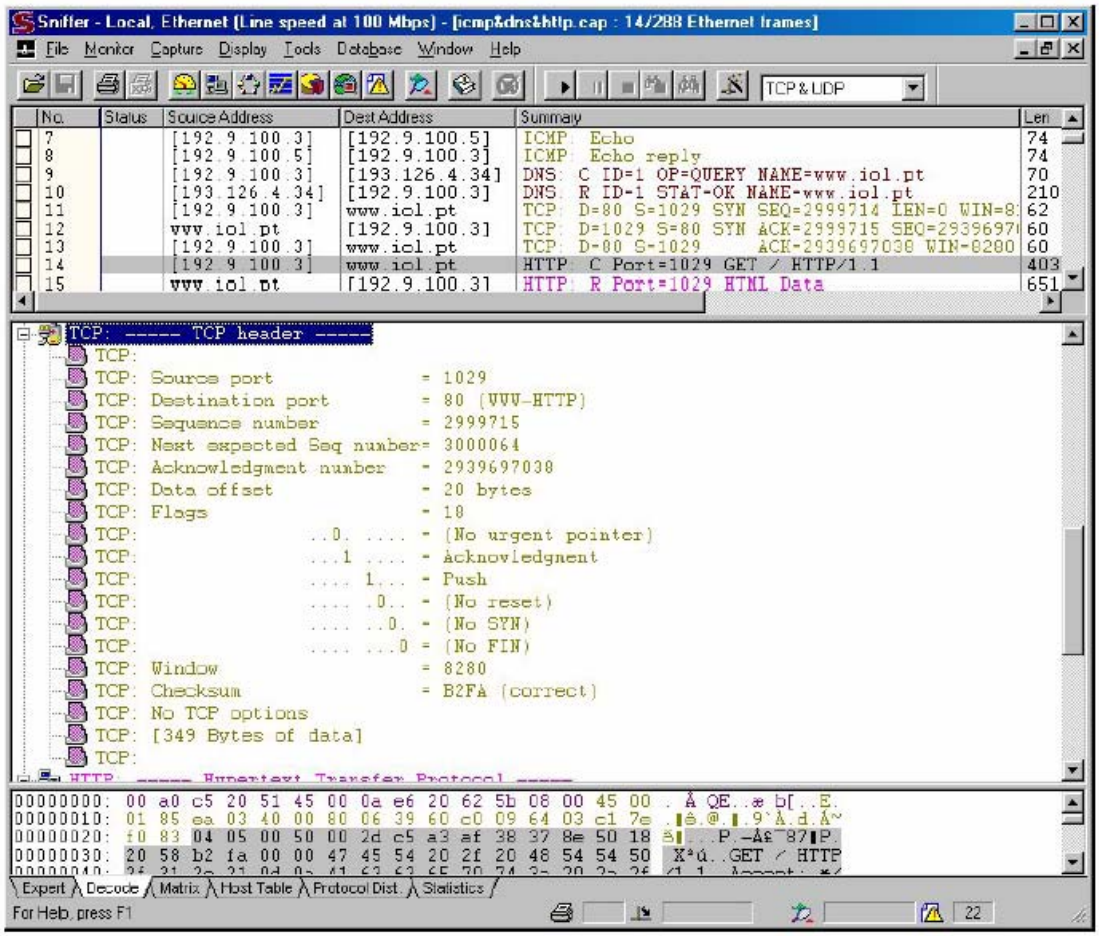
• *Flags* – Bits de controlo

• Janela – Especifica o tamanho da janela de recepção do destinatário, que serve para determinar qual o tamanho do grupo de tramas.

• *Checksum* – Para verificação da integridade da trama

• Opções – Podem-se especificar algumas opções de controlo na trama TCP

• Dados – Contém a informação recebida das camadas superiores.


Sniffer - Local, Ethernet (Line speed at 100 Mbps) - [icmp&dns&http.cap : 14/288 Ethernet frames]
File Monitor Capture Display Tools Database Window Help
TCP & UDP
No. Status Source Address Dest Address Summary Len
7 [192.9.100.3] [192.9.100.5] ICMP: Echo 74
8 [192.9.100.5] [192.9.100.3] ICMP: Echo reply 74
9 [192.9.100.3] [193.126.4.34] DNS: C ID=1 OP=QUERY NAME=www.iol.pt 70
10 [193.126.4.34] [192.9.100.3] DNS: R ID=1 STAT=OK NAME=www.iol.pt 210
11 [192.9.100.3] www.iol.pt TCP: D=80 S=1029 SYN SEQ=2999714 LEN=0 WIN=8 62
12 www.iol.pt [192.9.100.3] TCP: D=1029 S=80 SYN ACK=2999715 SEQ=2939697 60
13 [192.9.100.3] www.iol.pt TCP: D=80 S=1029 ACK=2939697030 WIN=8280 60
14 [192.9.100.3] www.iol.pt HTTP: C Port=1029 GET / HTTP/1.1 403
15 www.iol.pt [192.9.100.3] HTTP: R Port=1029 HTML Data 651
TCP: ----- TCP header -----
TCP:
TCP: Source port = 1029
TCP: Destination port = 80 (WWW-HTTP)
TCP: Sequence number = 2999715
TCP: Next expected Seq number= 3000064
TCP: Acknowledgment number = 2939697030
TCP: Data offset = 20 bytes
TCP: Flags = 18
TCP: ..0. .... = (No urgent pointer)
TCP: ...1 .... = Acknowledgment
TCP: .... 1... = Push
TCP: .... .0.. = (No reset)
TCP: .... ..0. = (No SYN)
TCP: ....0 = (No FIN)
TCP: Window = 8280
TCP: Checksum = B2FA (correct)
TCP: No TCP options
TCP: [349 Bytes of data]
TCP:
00000000: 00 a0 c5 20 51 45 00 0a e6 20 62 5b 08 00 45 00
00000010: 01 85 ea 03 40 00 80 06 39 60 c0 09 64 03 c1 7e
00000020: f0 83 04 05 00 50 00 2d c5 a3 af 38 37 8e 50 18
00000030: 20 58 b2 fa 00 00 47 45 54 20 2f 20 48 54 54 50
Expert Decode Matrix Host Table Protocol Dist. Statistics
For Help, press F1
22

Routers

Os routers são computadores dedicados a fazer o roteamento dos pacotes IP numa rede. Estes computadores utilizam a informação da camada 3 do protocolo TCP/IP para realizar esse roteamento. Os pacotes são então enviados para a rede de destino, podendo passar por vários *hops*.

Propriedades dos Routers

O roteamento consiste no acto de mover a informação entre redes, de uma rede de origem até uma rede de destino. Ao movimentar o pacote, o router não consegue determinar se o próximo salto é o router da rede de destino, e portanto o último, ou apenas mais um router no caminho.

Vários parâmetros são utilizados pelos routers de modo a determinar o caminho e estabelecer as rotas. O parâmetro mais importante é a **métrica**. A métrica é a unidade de medida padrão da qualidade da rota, e tem por base os tamanho e o atraso no canal. Para ajudar à determinação dos caminhos alternativos, existem algoritmos de roteamento que inicializam e mantêm tabelas de rotas. Estas tabelas contêm informação de roteamento que varia de acordo com o algoritmo utilizado.

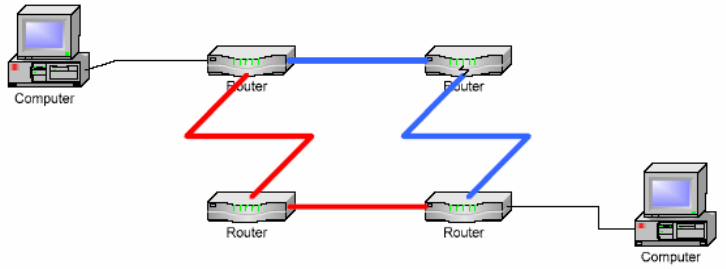
Na determinação dos caminhos, é utilizada uma associação nas tabelas de roteamento que indicam ao router que um determinado destino pode ser optimizado ao enviar o pacote para um determinado ponto na rede, um hop no caminho para o destino final. Ao receber um pacote, o router vai associar o destino através do endereço IP com a tabela de roteamento que lhe indica o próximo ponto para onde deve enviar o pacote. Os routers comparam a métrica para determinar as rotas óptimas. O caminho mais curto nem sempre é o melhor.

O processo de roteamento de pacotes consiste nos seguintes passos:

1. O pacote chega ao Router
2. Descarta a informação da camada 2
3. Após a obtenção do IP consulta as listas de acesso e permissões
4. Determina o caminho óptimo, com base nas tabelas de roteamento
5. Redirecciona o pacote para o próximo hop

Os routers também são capazes de redireccionar pacotes para outras redes que funcionem com outros protocolos, realizando neste caso uma conversão entre os protocolos em questão. São os chamados router multiprotocolo. Como exemplo, veja-se um router de acesso WAN, que liga directamente a uma LAN através do protocolo Ethernet, e à WAN (Internet) através de protocolos PPP e SLIP.

Uma outra propriedade dos routers é denominada de convergência. Esta propriedade faz com que os routers, se estiverem aptos a trabalhar com protocolos dinâmicos, substituam uma rota em falha por uma outra que garanta o correcto envio dos pacotes.



Protocolos de Roteamento

RIP

O RIP foi desenvolvido pela Xerox Corporation no inicio dos anos 80 para ser utilizado nas redes Xerox Network Systems (XNS), e, hoje em dia, é o protocolo intradominio mais comum, sendo suportado por praticamente todos os fabricantes de roteadores e disponível na grande maioria das versões mais actuais do sistema operacional UNIX.
Um de seus benefícios é a facilidade de configuração. Alem disso, seu algoritmo não necessita grande poder de computação e capacidade de memória em roteadores ou computadores.

O protocolo RIP funciona bem em pequenos ambientes, porem apresenta serias limitações quando utilizado em redes grandes. Ele limita o número de saltos (hops) entre hosts a 15 (16 é considerado infinito). Outra deficiência do RIP é a lenta convergência, ou seja, leva relativamente muito tempo para que alterações na rede fiquem sendo conhecidas por todos os roteadores. Esta lentidão pode causar loops de roteamento, por causa da falta de sincronia nas informações dos roteadores.

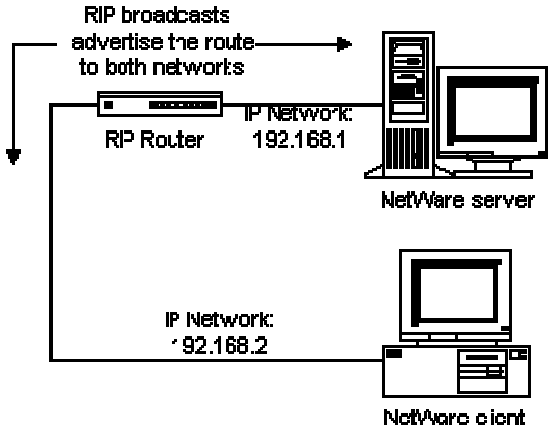
O protocolo RIP é também um grande consumidor de largura de banda, pois, a cada 30 segundos, ele faz um broadcast de sua tabela de roteamento, com informações sobre as redes e sub-redes que alcança.
Por fim, o RIP determina o melhor caminho entre dois pontos, levando em conta somente o número de saltos (hops) entre eles. Esta técnica ignora outros factores que fazem diferença nas linhas entre os dois pontos, como: velocidade, utilização das mesmas (tráfego) e toda as outras métricas que podem fazer diferença na hora de se determinar o melhor caminho entre dois pontos.

O protocolo RIP é uma directa implementação do roteamento vector-distância para redes locais. Em seu método de actuação ele divide as máquinas envolvidas em activas e passivas (silenciosas). Gateways activos informam suas rotas para outros, as máquinas passivas escutam e actualizam suas rotas baseadas nas informações, mas não informam. Tipicamente, gateways rodam RIP em modo activo, enquanto hosts usam modo passivo.

Um gateway rodando RIP no modo activo envia para a rede uma mensagem a cada 30 segundos, esta mensagem contém informações colhidas no banco de dados das rotas do gateway. Cada mensagem consiste de pares onde cada par contém um endereço IP de rede e uma distância da rede. RIP usa uma métrica de contagem de saltos para medir a distância ao destino. Na métrica RIP um gateway é definido para contar de um salto das redes conectadas directamente, de dois das que são alcançáveis através de outro gateway e assim por diante. O número de saltos contados ao longo de um caminho da origem ao destino, refere-se aos gateways encontrados neste.

Nem sempre o menor número de saltos significa a melhor rota, pode ser que uma rota mais longa propicie melhor qualidade de linhas. Para compensar esta diferença de tecnologia algumas implementações use alta contagem artificial de saltos quando informados de conexões lentas.

Participantes RIP, activos ou passivos ouvem todas as mensagens broadcast e actualizam suas tabelas de acordo com o algoritmo vector-distância.



Internet

Visualização e Pesquisa de Informação

Finger

O Finger é um comando de troca de informação sobre utilizadores. O protocolo descrito no RFC é um protocolo muito simples que permite aceder à informação sobre utilizadores de uma maquina remota. (o comando Finger também funciona numa maquina local, efectuando pedidos sobre utilizadores à própria maquina. Mas neste caso não é usado o protocolo de comunicação de redes)

De uma forma genérica o funcionamento do Finger resume-se a efectuar uma conexão à porta 79 do servidor, e a realizar um pedido. O servidor envia a resposta de acordo com os dados do pedido. Os dados enviados são em formato ASCII com os códigos de CR e LF no final.

Comunicação

Correio Electrónico

E-mail, **correio-e**, ou **correio electrónico**, ou ainda ***e-mail*** é um método que permite compor, enviar e receber mensagens através de sistemas electrónicos de comunicação. O termo *e-mail* é aplicado tanto aos sistemas que utilizam a Internet e são baseados no protocolo SMTP, como aqueles sistemas conhecidos como *intranets*, que permitem a troca de mensagens dentro de uma empresa ou organização e são, normalmente, baseados em protocolos proprietários.

O correio electrónico é anterior ao surgimento da Internet. Os sistemas de *e-mail* foram uma ferramenta crucial para a criação da rede internacional de computadores.

O primeiro sistema de troca de mensagens entre computadores que se tem notícia foi criado em 1965, e possibilitava a comunicação entre os múltiplos usuários de um computador do tipo *mainframe*. Apesar da história ser um tanto obscura, acredita-se que os primeiros sistemas criados com tal funcionalidade foram o Q32 da SDC e o CTSS do MIT.

O sistema electrónico de mensagens transformou-se rapidamente em um "*e-mail* em rede", permitindo que usuários situados em diferentes computadores trocassem mensagens. Também não é muito claro qual foi o primeiro sistema que suportou o *e-mail* em rede. O sistema AUTODIN, em 1966, parece ter sido o primeiro a permitir que mensagens electrónicas fossem transferidas entre computadores diferentes, mas é possível que o sistema SAGE tivesse a mesma funcionalidade algum tempo antes.

A rede de computadores ARPANET fez uma grande contribuição para a evolução do *e-mail*. Existe um relato que indica a transferência de mensagens electrónicas entre diferentes sistemas situados nesta rede logo após a sua criação, em 1969. O programador Ray Tomlinson iniciou o uso do sinal @ para separar os nomes do usuário e da máquina no endereço de correio electrónico em 1971. Considerar que ele foi o "inventor" do *e-mail* é um exagero, apesar da importância dos seus programas de *e-mail*: SNDMSG e READMAIL. A primeira mensagem enviada por Ray Tomlinson não foi preservada; era uma mensagem anunciando a disponibilidade de um *e-mail* em rede [2]. A ARPANET aumentou significativamente a popularidade do correio electrónico.

O envio e recebimento de uma mensagem de *e-mail* é realizada através de um sistema de correio electrónico. Um sistema de correio electrónico é composto de programas de computador que suportam a funcionalidade de cliente de *e-mail* e de um ou mais servidores de *e-mail* que, através de um endereço de correio electrónico, conseguem transferir uma mensagem de um usuário para outro. Estes sistemas utilizam protocolos de Internet que permitem o tráfego de mensagens de um remetente para um ou mais destinatários que possuem computadores conectados à Internet.

Newsgroup

Grupo de discussão que permite a troca pública de mensagens sobre os mais variados assuntos. Existem milhares deles na Internet. Os newsgroups são distribuídos através da Usenet e podem ser lidos acedendo a um servidor de "News" através de um software adequado para tal.

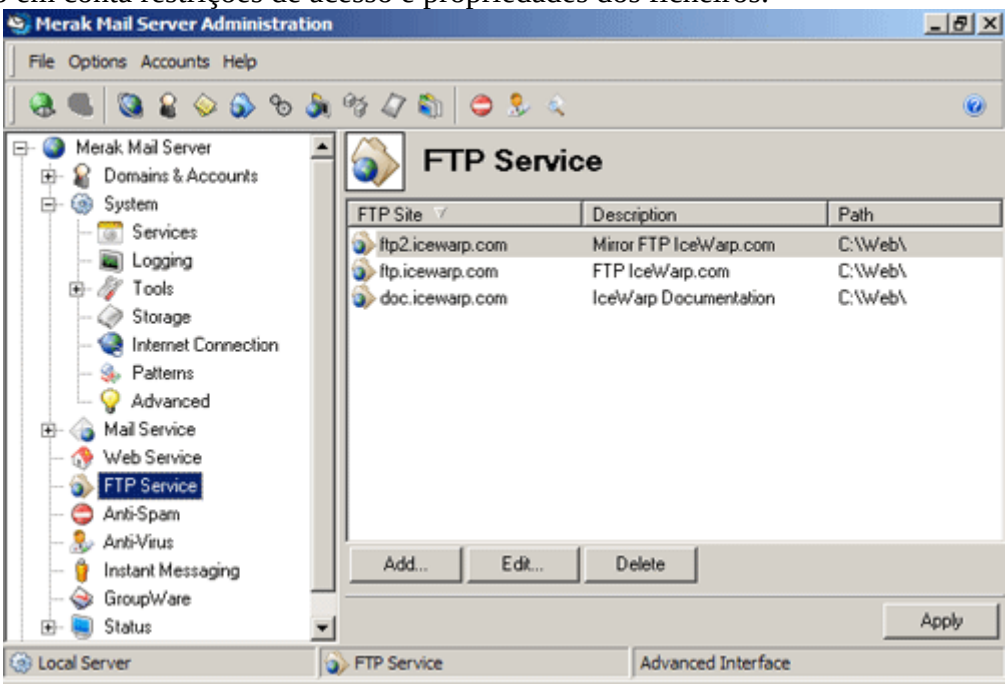
Usenet (do inglês *Unix User Network*) é um meio de comunicação onde usuários postam mensagens de texto (chamadas de "artigos") em fóruns que são agrupados por assunto (chamados de *newsgroups*). Ao contrário das mensagens de e-mail, que são transmitidas quase que directamente do remetente para o destinatário, os artigos postados nos newsgroups são retransmitidos através de uma extensa rede de servidores interligados.

O surgimento da rede data de 1979 e a maioria dos computadores participantes naquela época se comunicava através de conexões *discadas* por um protocolo chamado de UUCP, mas com a popularização da Internet nas décadas de 80 e 90 o sistema passou a funcionar quase que completamente baseado no protocolo NNTP da família de protocolos TCP/IP. O programa chamado INN é hoje o servidor mais utilizado para conectar as máquinas que fazem parte da rede Usenet.

Transferência de Ficheiros

FTP significa File Transfer Protocol (Protocolo de Transferência de Arquivos), e é uma forma bastante rápida e versátil de transferir arquivos (também conhecidos como ficheiros), sendo uma das mais usadas na Internet.
Pode referir-se tanto ao protocolo quanto ao programa que implementa este protocolo (neste caso, tradicionalmente aparece em letras minúsculas, por influência do programa de transferência de arquivos do Unix).

A transferência de dados em redes de computadores envolve normalmente transferência de ficheiros e acesso a sistemas de ficheiros remotos (com a mesma interface usada nos ficheiros locais). O FTP (RFC 959) é baseado no TCP, mas é anterior à pilha de protocolos TCP/IP, sendo posteriormente adaptado para o TCP/IP. É o standard da pilha TCP/IP para transferir ficheiros, é um protocolo genérico independente de hardware e do sistema operativo e transfere ficheiros por livre arbítrio, tendo em conta restrições de acesso e propriedades dos ficheiros.



Os nomes na Internet – DNS

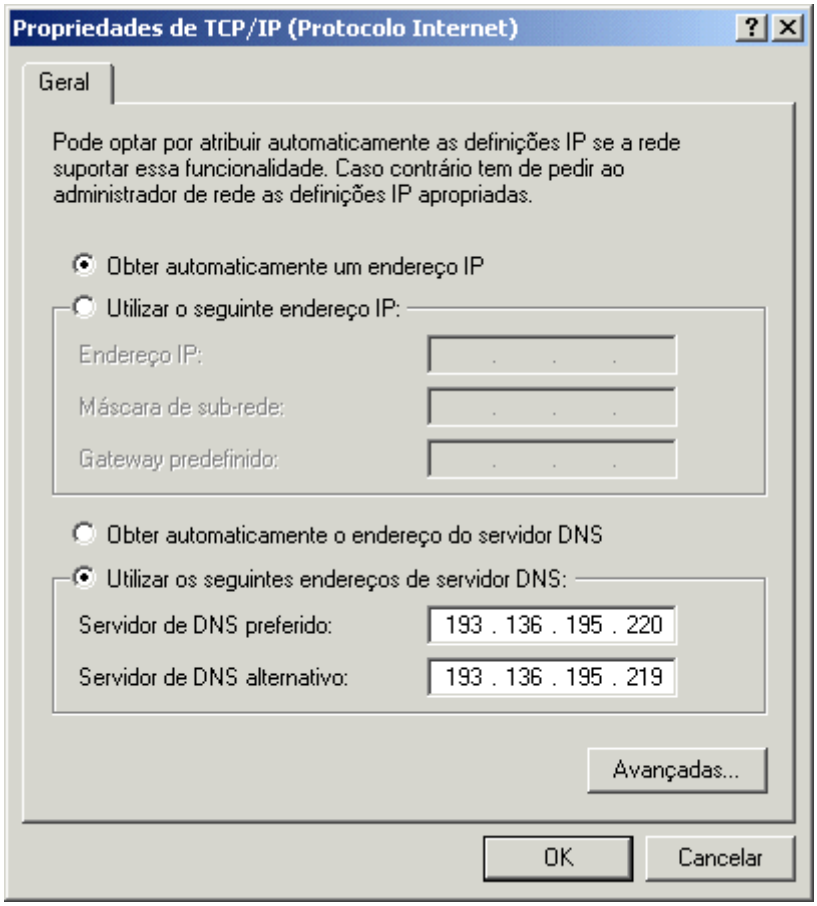
Endereçamento IP e Serviço de Nomes (DNS)

DNS (Domain Name Server — ou Servidor de Nomes de Domínio), consiste num servidor onde são armazenadas ligações entre IPs e domínios. Quando você pede ao seu navegador para chamar um determinado domínio, automaticamente ele acede ao servidor DNS configurado, e encontra o respectivo IP, a máquina que aloja aquela página (este processo não é usado apenas em páginas) e assim torna-se possível você aceder a sites usando nomes ao invés de números de IP.

Resolução de Nomes

Sendo este serviço fundamental para o normal funcionamento da Internet, torna-se imprescindível indicar aos computadores dos utilizadores o endereço IP do(s) servidor(es) de DNS a contactar para traduzir nomes em endereços numéricos e vice-versa.

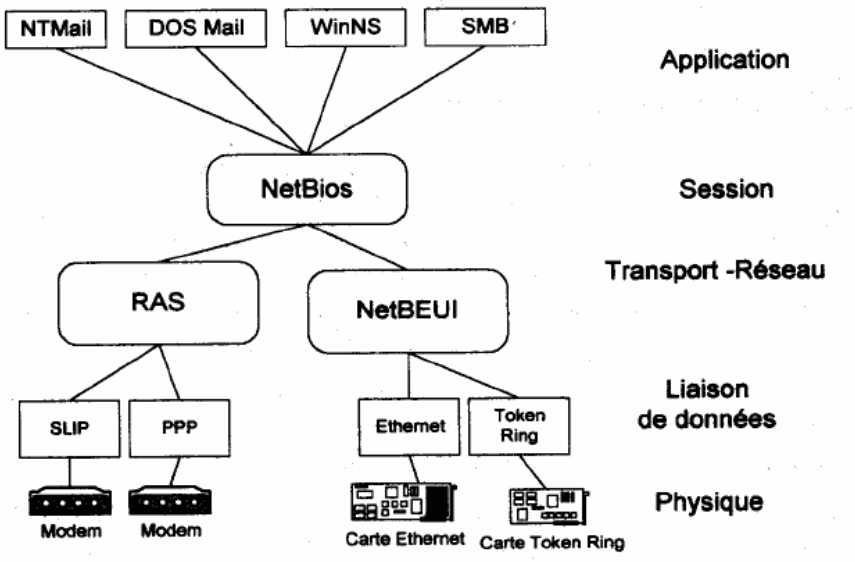
Esta operação é feita na configuração dos parâmetros TCP/IP da rede de cada computador.



NetBios

NetBIOS é uma interface de programa que foi desenvolvida para permitir a comunicação entre máquinas. Nesta estrutura foi implementado o conceito de nome de serviço, o que possibilita que uma máquina conecte-se à rede reservando um nome para sua utilização. Não há um servidor central para tratar os nomes definidos e qualquer máquina pode utilizar quantos nomes deseje, desde que ele não esteja em uso.
Esta arquitectura dinâmica tem sua origem em redes de PCs onde a instalação de um novo nó da rede deveria ser tão simples quanto possível, ou seja a configuração de uma máquina reduziu-se à definição de seu nome (ou quase isto). Problemas de duplicação de nomes, com um limite de 16 caracteres são insignificantes em redes de tamanho pequeno. Além do nome de serviço, existem ainda tarefas de comunicação, uma vez que os dados podem estar em formato seguro ou inseguro, o que pode ser comparado com os protocolos TCP e UDP do Unix. Os protocolos superiores como o SMB formam uma camada sobre o NetBIOS.

A interface NetBIOS pode ser implementada em diferentes arquitecturas de rede. Uma implementação que funciona relativamente próxima ao hardware chama-se NetBEUI, sendo muitas vezes referenciada como NetBIOS.
Para endereçamento de pacotes simples, NetBEUI utiliza o endereço de hardware do adaptador de rede. Ao contrário do IPX e endereços IP não é possível obter informações de roteamento através desta implementação, assim como pacotes NetBEUI não podem ser enviados através de um roteador, reduzindo a rede à uma actuação local, que necessita de bridges e repetidores para possíveis expansões.
TCP/IP e IPX são protocolos de rede que implementaram o NetBIOS, sendo que no TCP/IP ele é descrito nas RFCs 1001 e 1002.
Os nomes usados pelo NetBIOS não têm relação com os nomes usados em /etc/hosts/ ou os utilizados via DNS, porém é indicado utilizar a mesma denominação em ambos os métodos a fim de se evitarem confusões.

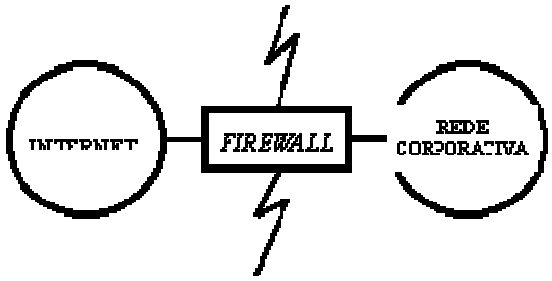


Segurança na Internet

Na Internet, como em qualquer outra sociedade, existe uma série de pessoas mal intencionadas que poderiam ser comparadas, na sociedade em que vivemos, aos furadores de muros, destruidores de caixas de correios ou simplesmente, pessoas que ficam nas ruas mexendo nos carros para ver o alarme disparar. Outro tipo de usuário que existe na Internet, está interessado em tirar o maior proveito possível dos benefícios que a Internet proporciona, principalmente no campo comercial e no campo da disseminação de informações. Muitos destes usuários são empresas, que possuem dados confidenciais que devem ser protegidos do acesso de pessoas não autorizadas.

Firewall

Firewall é um sistema ou grupos de sistemas que impõe uma política de controle de acesso entre duas redes. A princípio, o Firewall pode ser entendido como sendo composto de dois mecanismos distintos: um que bloqueia e controla qualquer tráfego que tenta da Internet passar para a rede corporativa, e outro que controla e permite que o tráfego da rede corporativa tenha acesso à Internet. Alguns Firewall dão uma maior ênfase para o bloqueio do tráfego que vem da Internet, outros dão uma maior ênfase para a permissão do tráfego que sai da rede corporativa e vai para a Internet.



O QUE UMA FIREWALL PODE PROTEGER ?

Alguns Firewall permitem que somente o tráfego de correio eletrônico passe por eles, protegendo a rede corporativa de qualquer ataque que venha a ser praticado sobre qualquer outro serviço disponível na Internet. Outros Firewall provêem um pouco menos de segurança, protegendo somente os serviços principais, onde os ataques mais comuns acontecem, tais como: telnet, ftp, finger, network file system (nfs), etc.

Firewall também são importantes do ponto de vista da auditoria de ataques, pois eles possuem uma série de registros que mostram todas as conexões que estão entrando ou saindo da rede corporativa, inclusive quais destas conexões foram bloqueadas. Um exemplo disto é quando um usuário hipotético tenta, via Telnet, aceder a uma máquina que está dentro de uma rede corporativa qualquer. Se esta rede estiver protegida por um Firewall, a conexão via Telnet será recusada e um registro será gerado mostrando a hora, o tipo da conexão, o endereço IP de quem tentou a conexão e qual foi o motivo pelo qual a conexão foi recusada. Com isto o administrador de segurança tem informações suficientes para fazer uma auditoria completa.

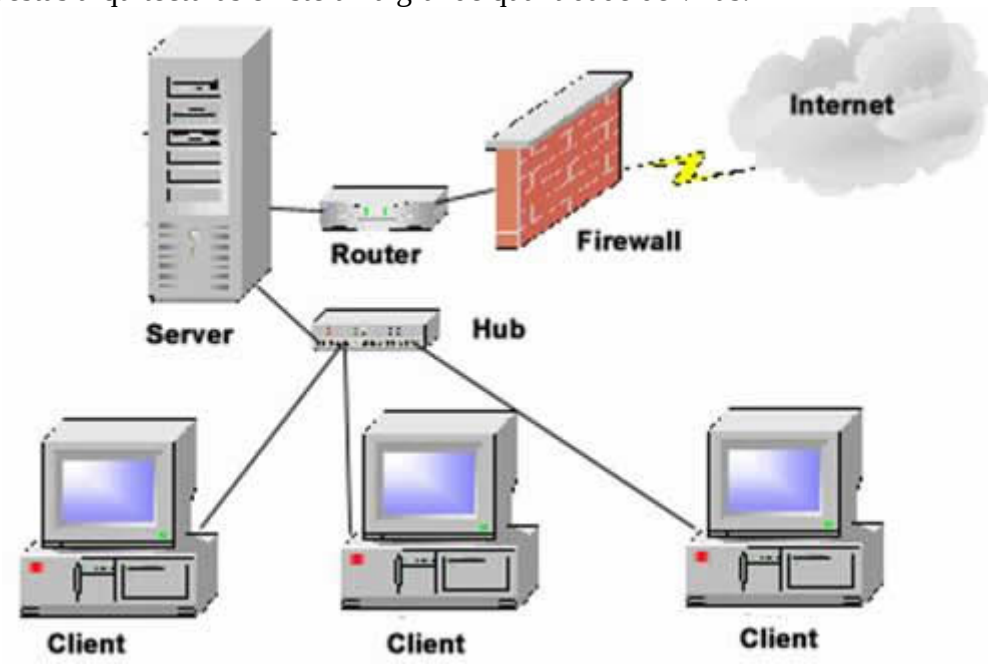
O QUE UMA FIREWALL NÃO PODE PROTEGER ?

Firewall não podem proteger ataques que não passam por ele. Muitas corporações têm um acesso à Internet controlado por um Firewall, mas também têm um acesso a sua rede corporativa através de linhas telefónicas discadas com modems, caracterizando a chamada porta dos fundos. O Firewall não impede que um ataque seja feito por esta linha telefônica, pois o tráfego de informações oriundos dos modems não passam pelos controles do Firewall.

Firewall também não protege contra pessoas mal intencionadas que estão dentro da organização, isto é, a pessoa que esta fazendo as ações contra a organização está sentada em uma máquina da própria organização. Enquanto uma organização protege suas informações dos acessos indevidos oriundos da Internet, uma pessoa da organização fornece as informações através de disquete, fax, telefone, etc.

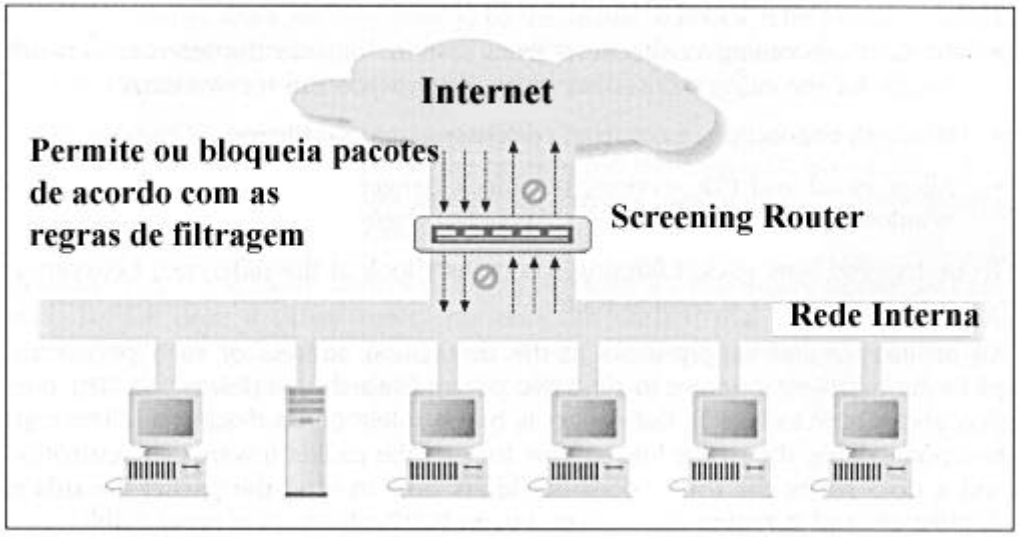
Firewall não protege contra pessoas que usam a informática mas não sabem muito bem como ela funciona, e quando tem dúvidas saem digitando qualquer comando ou tomando decisões sem saber muito bem o que vai acontecer.

Há uma série de maneiras de codificar códigos binários e transportá-los pela Internet, dificultando que algum Firewall consiga detectar se um vírus está ou não sendo descarregado por uma estação da rede corporativa. Um outro agravante é a grande quantidade de arquitecturas de hardware e software existentes, sendo que, para cada uma destas arquitecturas existe uma grande quantidade de vírus.



Filtragem de Pacotes

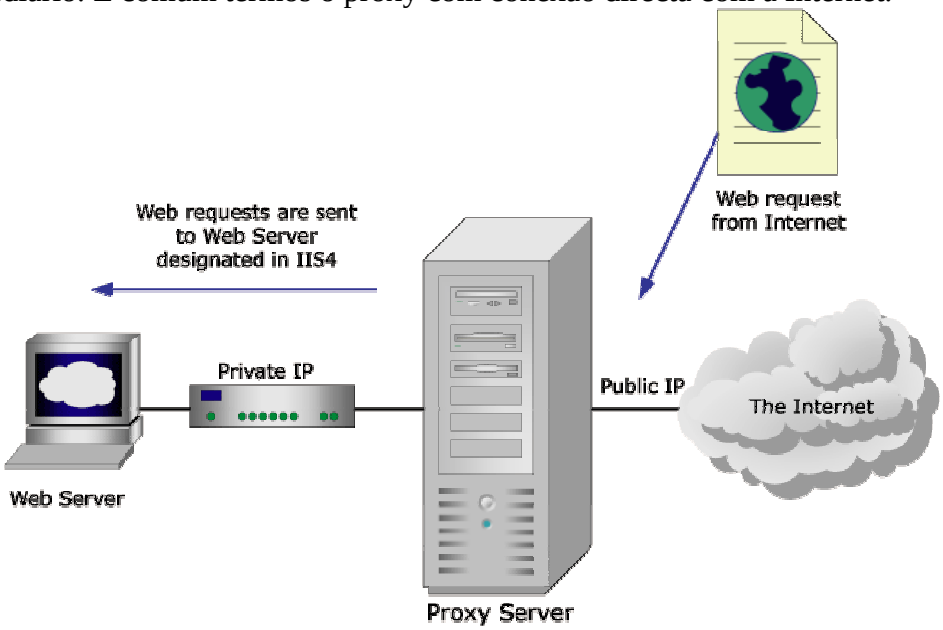
O Firewall que trabalha na filtragem de pacotes é muito utilizado em redes pequenas ou de porte médio. Por meio de um conjunto de regras estabelecidas, esse tipo de Firewall determina que endereços IPs e dados podem estabelecer comunicação e/ou transmitir/receber dados. Alguns sistemas ou serviços podem ser liberados completamente (por exemplo, o serviço de e-mail da rede), enquanto outros são bloqueados por padrão, por terem riscos elevados (como softwares de mensagens instantâneas, tal como o ICQ). O grande problema desse tipo de Firewall, é que as regras aplicadas podem ser muito complexas e causar perda de desempenho da rede ou não serem eficazes o suficiente.
Este tipo, se restringe a trabalhar nas camadas TCP/IP, decidindo quais pacotes de dados podem passar e quais não. Tais escolhas são regras baseadas nas informações endereço IP remoto, endereço IP do destinatário, além da porta TCP usada.
Quando devidamente configurado, esse tipo de Firewall permite que somente "computadores conhecidos troquem determinadas informações entre si e tenham acesso a determinados recursos". Um Firewall assim, também é capaz de analisar informações sobre a conexão e notar alterações suspeitas, além de ter a capacidade de analisar o conteúdo dos pacotes, o que permite um controle ainda maior do que pode ou não ser acessível.



Proxy

Um proxy é um software que armazena dados em forma de cache em redes de computadores. São instalados em máquinas com ligações tipicamente superiores às dos clientes e com poder de armazenamento elevado.
É de salientar que, utilizando um proxy, o endereço que fica registrado nos servidores é o do próprio proxy e não o do cliente.
Por exemplo, no caso de um HTTP caching proxy, o cliente requisita um documento na World Wide Web e o proxy procura pelo documento em seu cache. Se encontrado, o documento é retornado imediatamente. Senão, o proxy busca o documento no servidor remoto, entrega-o ao cliente e salva uma cópia no seu cache.
A tradução da palavra inglesa proxy, segundo o dicionário Michaelis, significa procurador, substituto ou representante.

O proxy surgiu da necessidade de conectar uma rede local à Internet através de um computador da rede que compartilha sua conexão com as demais máquinas. Em outras palavras, se considerarmos que a rede local é uma rede "interna" e a Internet é uma rede "externa", podemos dizer que o proxy é que permite outras máquinas terem acesso externo. Geralmente, máquinas da rede interna não possuem endereços válidos na Internet e, portanto, não têm uma conexão directa com a Internet. Assim, toda solicitação de conexão de uma máquina da rede local para um host da Internet é direccionada ao proxy, este, por sua vez, realiza o contacto com o host desejado, re-passando a resposta à solicitação para a máquina da rede local. Por este motivo , é utilizado o termo proxy para este tipo de serviço, que é traduzido para procurador ou intermediário. É comum termos o proxy com conexão directa com a Internet.



Desvantagens:

• Para cada novo serviço que aparece na Internet, o fabricante deve desenvolver um o seu correspondente agente de Proxy. O que pode demorar meses, tornando o cliente vulnerável enquanto o Fabricante não libera o Agente. A instalação, manutenção e upgrade dos agentes de Proxy requerem serviços especializados de gestão da Firewall e podem ser bastante caros.

• Os proxies introduzem perda de performance na rede, já que as mensagens devem ser processadas duas vezes, pelo gateway e pelo agente de Proxy. Por exemplo, o serviço FTP manda um pedido ao agente de Proxy para FTP, que por sua vez fala com o servidor interno de FTP para completar o pedido.

• Os gateways são caros e requerem estações UNIX, que não são baratas, implicando ainda em multiplicação de sistemas operacionais, o que pode afectar toda a arquitectura da informática ou o seu Plano Director.