Licenciatura em Engenharia Electrónica Industrial

Laboratórios Integrados III

Módulo de redes de computadores

Texto de apoio

versão 04/05

Paulo Cardoso

Departamento de Electrónica Industrial

Índice

Introdução

Nos primeiros tempos dos computadores, as organizações tinham um grande computador com vários terminais, através dos quais os utilizadores trocavam informação com o sistema.. Isto foi uma grande revolução para as organizações.

No entanto rapidamente se começou a perceber não bastava ter um computador, era também necessário poder trocar informação com outros computadores. Esta necessidade, aliada à vulgarização dos computadores levou à grande expansão que as redes informáticas têm actualmente. As redes de computadores servem para trocar informação e partilhar recursos. Podem ir de redes que abrangem uma sala até redes intercontinentais.

A abordagem aqui feita às redes de computadores pretende ser apenas introdutória e serve como apoio ao módulo de redes da disciplina da Laboratórios Integrados III. Como tal vamo-nos cingir primordialmente à tecnologia que esteja à disposição na sala de aula.

Pretende-se desta forma criar alguma familiaridade com as tecnologias de rede, desde a utilização, passando pela instalação física da rede e de aplicações e, indo até à observação de interacções e da forma como estas se processam.

Parte I - Os protocolos

Nesta parte vamos discutir tudo aquilo que é transparente para o utilizador, que é toda a infra-estrutura de suporte da rede.

Após uma introdução de conceitos usando o modelo OSI, vamos abordar os vários níveis de um sistema de comunicação, enquadrando-os em implementações existentes.

1 O modelo OSI

Um sistema de comunicação é bastante complexo. Por isso, a ISO, International Standard Organization, definiu, em 1983, um modelo de referência subdividindo o sistema em vários sub-sistemas. Este modelo é chamado de modelo OSI, Open Systems Interconnection, tal como apresentado na figura 1.

Fig. 1 O modelo de referência OSI

Através deste modelo, o problema complexo da comunicação entre computadores é dividido em vários sub-problemas de menor complexidade. Obtém-se assim uma estrutura por camadas em que cada camada endereça um problema bem definido. Desta forma, segmentando as tarefas que cada camada executa, é possível alterar uma das camadas com pouco ou nenhum impacto nas outras. Por outro lado, tal como o nome indica, este é o modelo para a interligação de sistemas abertos. O que se passou durante muito tempo é que cada fabricante de computadores tinha o meu modelo e as suas normas na interligação de computadores, criando assim sistemas fechados que apenas "falavam" entre máquinas do mesmo fabricante. O modelo de referência facilita a criação de um conjunto de serviços para cada uma das camadas, que permite a comunicação entre dois sistemas quaisquer.

1.1 O conceito de serviço

Pelo que acabou de ser dito, verifica-se que a cada camada estão associadas um conjunto de serviços. Um serviço representa um conjunto de funcionalidades oferecidas por um determinado nível e é formado à custa da comunicação entre duas entidades e da utilização que fazem dos serviços da camada inferior. A comunicação entre as duas entidades é feita à custa de um conjunto de regras. Esse conjunto de regras designa-se por protocolo.

Desta forma, cada nível oferece os seus serviços ao nível imediatamente acima e utiliza os serviços do nível inferior. Um determinado nível torna os seus serviços disponíveis através dos *service acess points*, SAPs. A figura 2 exemplifica este relacionamento.

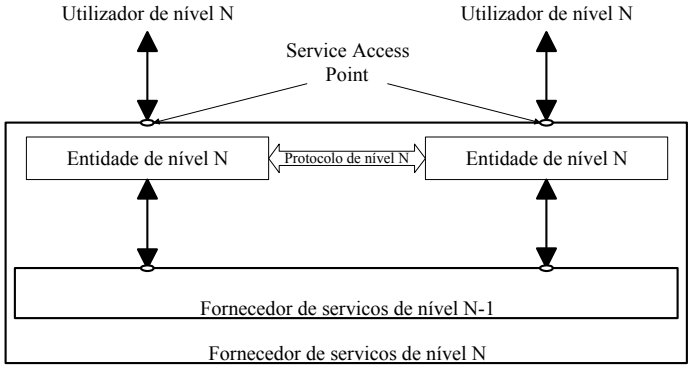


Fig. 2 Conceito de serviço no modelo OSI

Vejamos o seguinte exemplo:

> "O João pretende enviar uma carta ao António. Para isso preenche a carta e dá-a ao carteiro A. Este leva a carta à central α dos correios, que a encaminha para a central β, onde o carteiro B a recolhe e entrega ao António."

Em função deste exemplo pode-se redesenhar a figura anterior:

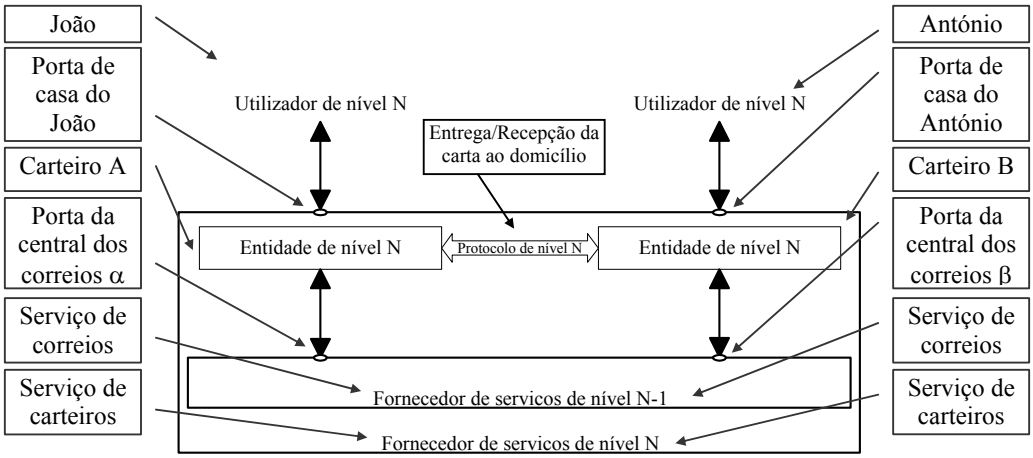


Fig. 3 Exemplo do conceito de serviço no modelo OSI

Como se vê por este exemplo, os carteiros só por si não valiam de nada pois não teriam quem encaminhasse a carta, por isso utilizam os serviços de encaminhamento de cartas fornecido pelos correios. Por outro lado os correios não passam sem os carteiros pois são estes que lhes entregam e recolhem as cartas. Temos assim várias tarefas bem delimitadas e interdependentes.

Através deste exemplo, podemos que a comunicação se passa em duas direcções:

- na horizontal: Num determinado nível as entidades envolvidas cooperam, usando um conjunto de regras, para que um tipo de serviço seja oferecido. Essas regras são chamadas de protocolo. Cada nível tem o seu protocolo. Neste caso o protocolo usado entre os carteiros é básico e a comunicação entre as entidades é mínima. Mas a

comunicação já seria maior se o carteiro A quisesse que o carteiro B o informasse de que a carta chegou ao destino. Esta comunicação não é directa mas sim através da comunicação que se passa na vertical;
- na vertical: o João entrega a carta ao carteiro, este entrega-a aos correios, etc. Como se vê a informação, neste caso a carta, vai descendo vários níveis, fazendo depois o percurso inverso.

1.2 Primitivas dos serviços

A figura 4 apresenta a generalização deste modelo. Além disso pode-se ver que a comunicação entre um utilizador e o seu fornecedor de serviços é feita utilizando um conjunto de primitivas.

As primitivas são:

- service-N.REQUEST. Usada quando o utilizador requisita o serviço "service" ao fornecedor de serviços de nível N;
- service-N.INDICATION. Usada pelo fornecedor de serviços de nível N para indicar ao utilizador remoto que o serviço "service" foi requisitado, ou então para reportar um evento;
- service-N.RESPONSE. Resposta do utilizador remoto ao fornecedor de serviços de nível N, relativa à primitiva anterior;
- service-N.CONFIRM. Resposta do fornecedor de serviços de nível N ao serviço requisitado pelo utilizador.

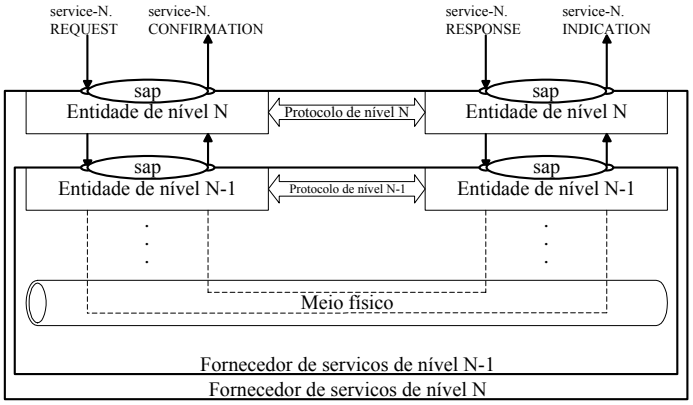


Fig. 4 Comunicação e o modelo OSI

Como exemplo deste modelo, uma ligação telefónica entre o João e o António teria a seguinte forma:

CONNECT.REQUEST	O João marca o número do António;
CONNECT.INDICATION	O telefone do António toca;
CONNECT.RESPONSE	O António atende;
CONNECT.CONFIRM	O João nota que alguém atendeu;
DATA.REQUEST	O João começa a falar;
DATA.INDICATION	O António ouve as palavras do João;
DATA.REQUEST	O António responde;
DATA.INDICATION	O João ouve as palavras do António;
DISCONNECT.REQUEST	O João desliga;
DISCONNECT.INDICATION	O António nota o sinal de desligado e faz o mesmo;

1.3 Tipos de serviço

A implementação destas primitivas é normalmente feita à custa de funções com os respectivos parâmetros. As primitivas são usadas em função do serviço usado. Estes pode ser confirmado, não confirmado, local e iniciado pelo fornecedor.

A figura 4 representa um serviço confirmado. Neste tipo de serviços, é recebida uma resposta é recebida uma resposta por parte do utilizador remoto. A figura 5 representa uma outra forma de representar um serviço confirmado.

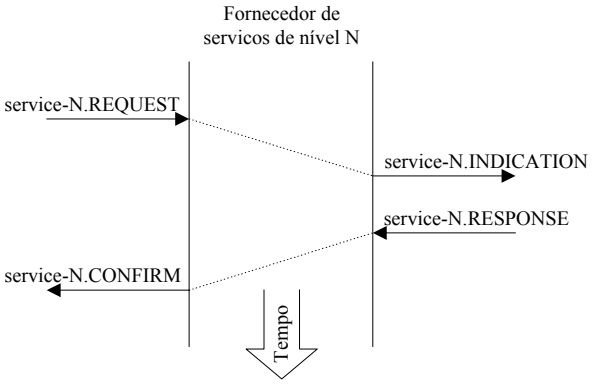


Fig. 5 Serviço confirmado

Num serviço não confirmado, tal como o nome indica, não há confirmação à origem de que o serviço foi indicado à entidade remota. Na figura 6 é apresentada a representação de um serviço não confirmado.

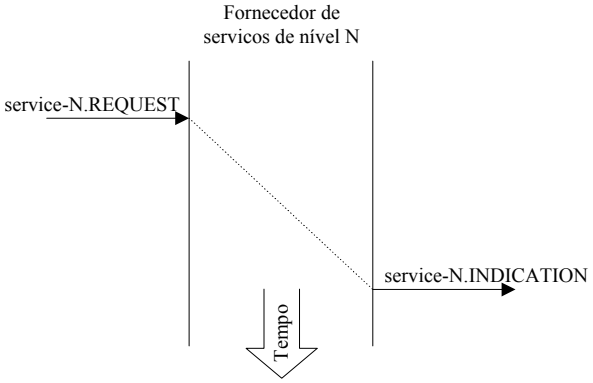


Fig. 6 Serviço não confirmado

Um utilizador pode requisitar um serviço que não tenha repercussões no utilizador remoto. A exemplificação deste tipo de serviço é feita através da figura 7.

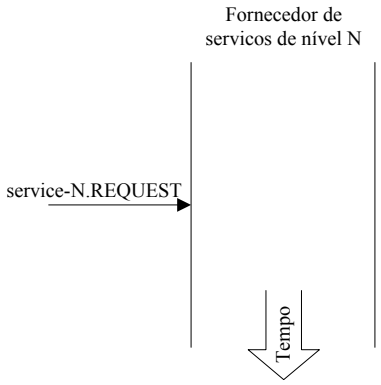


Fig. 7 Serviço local

Um outra situação tem a ver com a indicação de um evento a um utilizador, por parte do fornecedor de serviços, tal como é representado pela figura 8.

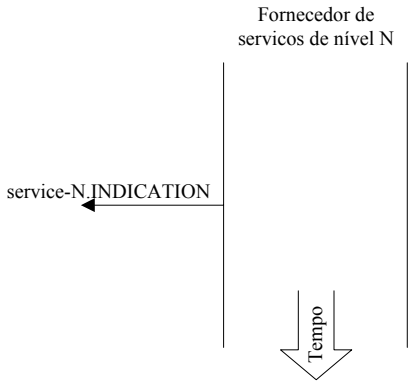


Fig. 8 Serviço iniciado pelo fornecedor

Uma outra característica dos serviços tem a ver com o facto de estes poderem ser ou não orientados à conexão. Assim temos:

- Serviços orientados à conexão: serviços através dos quais é criado um canal de comunicaçãovirtual entre duas entidades. Estes serviços são caracterizados por três fases: o estabelecimento de conexão, a troca de informação e a libertação da conexão;
- Serviços não orientados à conexão: neste tipo de serviços não há estabelecimento de conexão.

Podemos assim ter a combinação de vários tipos de serviços, apresentados na tabela 1.

Serviço	Exemplo
Serviços orientados à conexão confirmados	Fax
Serviços orientados à conexão não confirmados	Telefone
Serviços não orientados à conexão confirmados	Carta com aviso de recepção
Serviços não orientados à conexão não confirmados	Carta

Tab. 1 Tipos de serviços

1.4 A transferência de informação

Como anteriormente foi referido, a informação circula, no emissor, dos níveis superiores para os inferiores, passa por um meio físico e no sentido inverso no receptor. No entanto, para implementar o protocolo de comunicação entre as entidades de uma camada, a comunicação na horizontal, é necessário acrescentar informação, que não é passada à camada superior. Desta forma, aquando do envio, em cada nível é acrescentado um cabeçalho à informação que é recebida do nível superior. O conjunto resultante forma um pacote do protocolo usado na interacção. Na recepção, a camada correspondente retira o cabeçalho à informação. , A figura 9 apresenta a esquematização desta comunicção.

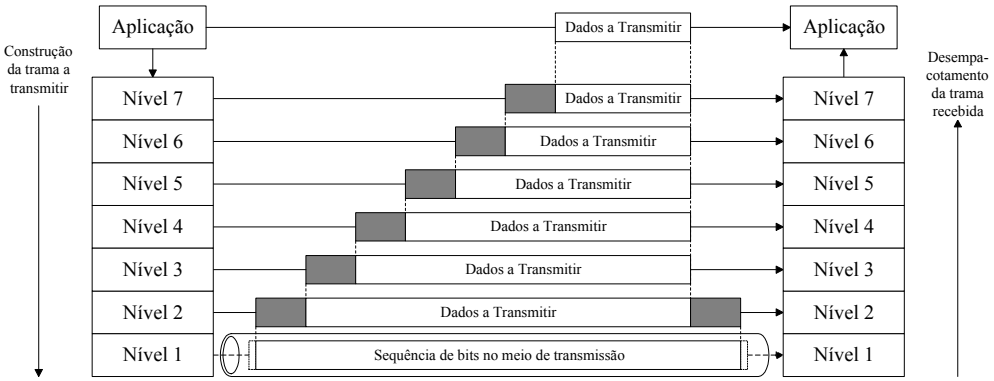


Fig. 9 A formação dos pacotes de dados em cada um dos níveis

2 O nível físico

Esta camada refere-se à forma como a informação circula no canal de comunicação, tratando questões tais como:

- Características mecânicas: tipo de conector;
- Caraterísticas electricas: nível eléctrico dos *bits* e sua codificação;
- Características funcionais: descrição do *pinout* dos conectores;
- Características pocedimentais: sequência legal de eventos (tipo de transmissão, síncrona ou assíncrona; modo de transmissão, *full-duplex*, *half-duplex*, *simplex*; etc)

Dois PCs ligados entre si através da porta série, tal como mostra a fig. 10, formam um sistema básico de comunicação, em que a norma EIA RS232 C define um protocolo de nível físico, tal como outras normas que definem sofisticados protocolos para redes locais. O *software* que usamos para transferir dados neste ambiente implementa, de uma forma consciente ou não, alguns dos níveis superiores da pilha OSI.

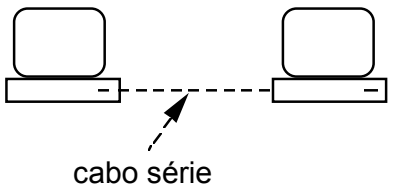


Fig. 10 Ligação série entre dois equipamentos

Se um sistema de comunicações se ficasse apenas por este tipo de interligações seria

limitado, pelo que embora estas ligações ponto a ponto sejam muito importantes, especialmente para a interligação de redes, o que se encontra mais vulgarmente numa rede local é um meio de comunicação que interliga vários equipamentos.

2.1 Topologia

A forma como vários equipamentos estão interligados define a sua topologia.
As topologias mais conhecidas são:

- barramento;
- estrela;
- anel.

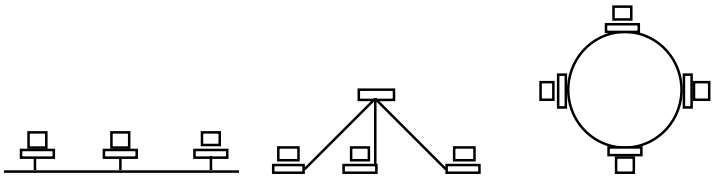


Fig 11 Topologias

É necessário distinguir dois tipos de topologias:

- Topologias lógicas;
- Topologias físicas.

Por exemplo, em certo tipo de redes lógicas a informação circula em forma de anel, de uma estações para as outras, embora as estações estejam fisicamente num barramento.
Neste momento apenas nos vamos debruçar sobre as topologias físicas.
Os dois protocolos mais conhecidos de redes locais são:

- Ethernet, que usa uma topologia em barramento;
- Token-ring, que usa uma topologia em anel.

No entanto quer o Ethernet, quer principalmente o Token-ring, podem assumir uma topologia em estrela. Isto deve-se a equipamentos chamados **concentradores**, ou *hubs*, para a rede Ethernet e, as **MAUs**, *Multistation Access Units*, no Token-ring.
Nestes equipamentos, tal como se pode ver pela fig. 12, o barramento, ou o anel, é implementado pelo *hardware* do equipamento.

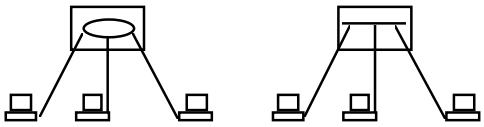


Fig 12 Configurações em estrela

2.2 Uma rede baseada em Ethernet

Vamos usar a rede Ethernet como exemplo, pois é a mais utilizada. No entanto os princípios aplicam-se a outros tipos redes.

A norma Ethernet é uma norma *de facto*, isto é, é uma norma de um conjunto de fabricantes que se tornou um *standard* devido à sua grande aceitação pelo mercado. As normas *de jure*, são aquelas que são estabelecidas por organizações internacionais, tais como ISO, ITU (ex-CCITT), etc.

O Ethernet foi criado nos anos 70 pela Xerox. Esta norma define uma rede em barramento utilizando cabo coaxial. Seguidamente formou-se um grupo constituído por DEC, INTEL e XEROX, daí vem o acrónimo DIX, para promover este novo produto.

Em 1985 foi criada uma nova versão do Ethernet, o Ethernet II, que é o que ainda hoje é usado.

Entretanto, o IEEE, *Institute of Electrical Electronics Engineers*, decidiu normalizar, através do projecto 802, várias tecnologias para redes locais, tendo, devido ao seu grande sucesso, usado o Ethernet II como base para a sua norma 802.3.

Existem assim actualmente como que duas normas Ethernet, o DIX Ethernet, ou Ethernet II, e o 802.3 Ethernet. Estas duas normas são muito parecidas, sendo em muitos casos os termos usados indistintamente.

Na fig. 13 vemos um exemplo de uma instalação baseada em Ethernet.

Neste caso existe um cabo Ethernet fino ao qual estão ligadas várias máquinas. Está também ligado a esse cabo um *hub*.

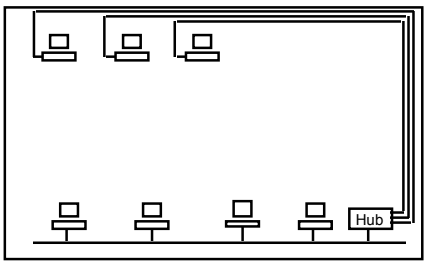


Fig 13 Exemplo de uma instalação

Nesta instalação existem dois tipo de cablagem, o cabo coaxial Ethernet fino, à qual estão ligadas directamente as estações de trabalho, e o cabo UTP que liga outras estações ao *hub*. A função do *hub* é a de servir de concentrador de cablagem UTP. Neste tipo de instalação tem que existir um cabo por estação. Temos assim uma estrutura mista, barramento e estrela.

2.2.1 O cabo coaxial

A norma Ethernet especifica que pode ser usada sobre dois tipos de cablagem coaxial. Essas especificações definem os chamados cabos Ethernet fino, RG 58A/U ou C/U, e cabos Ethernet grosso, RG 8A/U. Também são chamados, nas normas IEEE, de 10Base2 e 10Base5, respectivamente. ***10*** de 10Mb/s, taxa de transmissão; ***Base*** de Baseband, tipo de modulação do sinal; ***5*** de tamanho máximo do segmento em centenas de metros.

O cabo Ethernet fino é cabo coaxial flexível com um diâmetro de cerca de 0,5 cm. Para inserir uma estação na rede é necessário seccionar um segmento sendo a ligação à estação feita através de um conector em forma de T. As estações podem ser inseridas, ao contrário do cabo grosso, em qualquer ponto do cabo. Nas extremidades o cabo deve estar terminado, com cargas de 50 Ohm.

Cada segmento 10Base2 deve respeitar as seguintes características:

- Comprimento máx.:185 m;
- Nº máx. de estações p/ segmento: 30;
- Distância mínima entre cada estação: 0,5 m.

O cabo Ethernet grosso é um cabo rígido, com cerca de 1 cm de diâmetro, geralmente de cor amarela. Só se deve inserir estações na rede nos pontos indicador no cabo por marcas pretas.

Para inserir uma estação na rede é necessário usar equipamentos chamados *transceivers*. Como se pode ver pela fig. 14, a cabeça do *transceiver* entra em contacto com a malha externa e núcleo do cabo. Este *transceiver* tem cabeça do tipo vampiro, isto por oposição ao tipo T, em que a cabeça do *transceiver* tem um conector do tipo T, para ligar a um cabo Ethernet fino. Sim, também se podem usar *transceivers* em cabo Ethernet fino.

O *transceiver* tem uma porta DB15, porta AUI, para ligação através de um cabo, ao equipamento terminal.

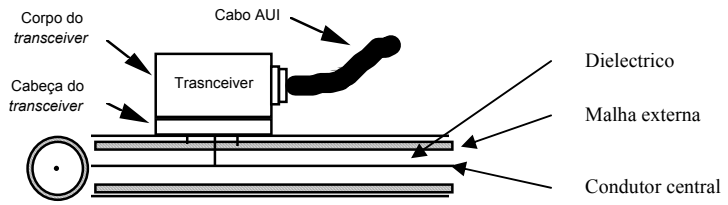


Fig 14 O *transceiver* no cabo 10Base5

Cada segmento 10Base5 deve respeitar as seguintes características:

- Comprimento máx.:500 m;
- Nº máx. de estações p/ segm.: 100;
- Tam. máx. cabo AUI: 50m;
- Dist. mín. entre cada estação: 2,5 m.

De referir ainda que o nº máximo de segmentos Ethernet que uma rede pode ter, separados por repetidores é de 4, sendo um deles apenas para interligação entre repetidores.

2.2.2 O cabo UTP

O cabo UTP, *Unshielded Twisted Pair*, é um cabo que contém 4 pares trançados, do género dos usados nas cablagens telefónicas. É dividido em 3 categorias, categoria 3, 4 e 5, tal como apresentado na tabela 2.

Tipo de cabo	Utilização comum
Categoria 1	Serviço telefónico e dados de baixa velocidade. Era usado para cablagens telefónicas antes dos anos 80. Não está certificado para o transporte de dados
Categoria 2	Dados até 1Mhz. Usado para instalações de RDIS. É popular em algumas instalações antigas de Token Ring. Utilizado para transporte de dados até 4Mbps.
Categoria 3	Dados até 16Mhz. Usado principalmente nas instalações Ethernet mais antigas. Utilizado por 10BaseT a 10Mbps e 100BaseT4 a 100Mbps.
Categoria 4	Dados até 20 MHz. Usado por Token Ring a 16Mbps e 100BaseT4 a 100Mbps.
Categoria 5	Dados até 100Mhz. Usado por 100BaseTX e 100BaseT4 a 100Mbps.

Tab 2 Categorias do cabo UTP e suas aplicações

Existem também o chamado STP, Shielded Twisted Pair, e o FTP, Foiled Twisted Pair, que também são usados para cablagens de dados.

O Ethernet 10BaseT, corre em cabos UTP nível 3. No entanto e porque o cabo de nível 5 suporta velocidades até 100Mb/s, é muito usado, deixando assim uma folga para um eventual *upgrade* para redes mais rápidas.

Estes cabos são usados para ligações em estrela, tal como se viu na fig. 13, em que cada cabo representa uma ligação pontoa ponto entre a estação de trabalho e o *hub*.

A única restrição associada a esta cablagem é a distancia entre estação e *hub* que não deve ser superior a 100m.

Este tipo de cablagem ganha cada vez mais adeptos por várias razões. Uma delas é a de que acabam os problemas dos outros tipos de Ethernet, em que uma falha num cabo deita abaixo toda a rede. Com esta estrutura em estrela todas as estações estão ligadas individualmente ao *hub*. Se este detecta uma falha numa estação a ligação a essa estação é desactivada.

Uma outra razão da utilização desta cablagem é a modularidade. Actualmente em muitos edifícios existe a chamada "calha técnica", e que não é mais do que uma calha, muitas vezes de plástico, que acompanha todas as paredes das salas, geralmente ao nível do chão e onde em qualquer ponto se pode criar uma tomada, seja de corrente eléctrica, seja de telefone ou de computador. O que muitas vezes se faz nesses edifícios é instalar tomadas RJ45 ao longo da calha, indo toda a cablagem dessas tomadas pela calha até painéis de distribuição. A modularidade desta solução está na possibilidade de se poder ligar às tomadas RJ45, existentes junto dos utilizadores, um telefone, um terminal, um computador, etc. É no painel de distribuição é que se selecciona a funcionalidade da tomada, ligando a saída a uma linha telefónica, a um servidor de terminais, a um hub, etc. A este tipo de infra-estrutura dá-se o nome de cablagem estruturada.

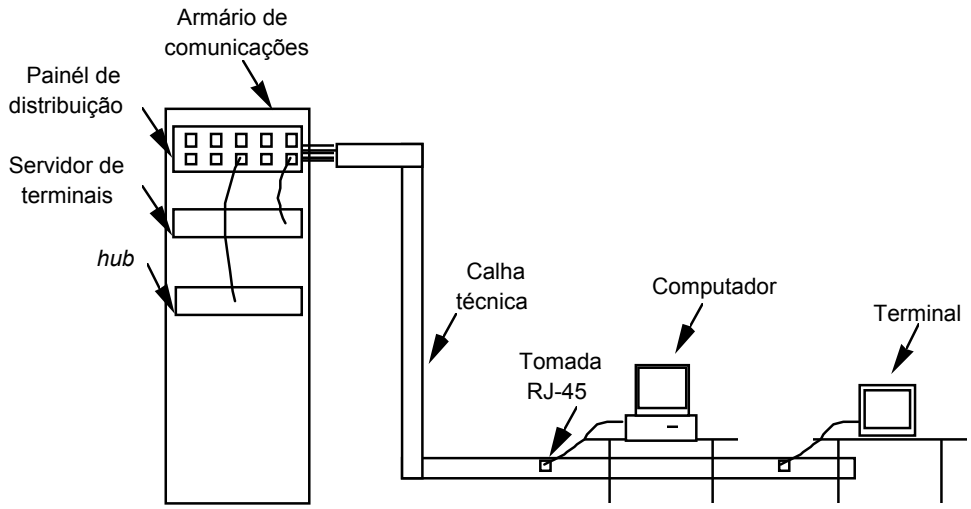


Fig 15 Exemplo de um sistema de cablagem estruturada

2.2.3 A fibra óptica

A fibra óptica é uma tecnologia que só recentemente passou a ser vulgarmente usada na transmissão de dados, isto devido principalmente a seu custo. É formada por um núcleo rodeado por uma camada chamada de *cladding*. Ambos são em vidro mas com diferentes índices de refracção, a luz atravessa o núcleo sendo reflectida pelo *cladding*. A fibra é protegida, no seu exterior, por uma pequena camada de plástico, para protecção.

Existem basicamente dois tipos de fibra:

- monomodo. Especificada para a utilização de apenas um comprimento de onda da luz, tendo assim menos perdas, sendo no entanto mais cara. Tipicamente as fibras têm diâmetro de 8 μm de núcleo e 125 μm de *cladding*;
- multimodo. É baseada na possibilidade de combinar diferentes comprimentos de

onda na mesma fibra, tendo, no entanto mais perdas, menor desempenho, mas é mais barata. Tipicamente as fibras têm diâmetro de 62,5μm de núcleo e 125 μm de *cladding*.

A ligação de duas fibras é feita basicamente ou mecanicamente ou por fusão. O primeiro caso, mais barato, é mais sujeito a perdas. No segundo caso, as pontas das fibras são fundidas uma contra a outra.

Os conectores que são usados pelas fibras são um dos seguintes: ST, SC, FC, MIC, SMA.

Actualmente devido à diminuição do seu preço, cada vez mais a fibra óptica é utilizada, sendo também usada nas redes Ethernet com a norma 10BaseFL. Esta norma define segmentos de até 2000m. Nestas redes a fibra óptica é basicamente utilizada para fazer a interligação de segmentos entre edifícios ou para servir de espinha dorsal da rede. Apenas um par de fibra é necessário. Os conectores especificados são do tipo SC.

Com o aparecimento de redes de maior desempenho a fibra óptica passou a ser requisito para a espinha dorsal da rede.

2.2.4 Teste da instalação

Após a instalação, ou durante a operação normal, poderá ser necessário testar as cablagens. O primeiro e dispositivo de deste mais básico é o multímetro. Com este equipamento pode-se ver, por exemplo, se há curto-circuitos, circuitos abertos, existem as cargas de 50Ω. Um teste simples poderá ser, após a instalação da cablagem, verificar numa ponta de um cabo 10Base2 a resistência entre malha externa e o condutor interno. O resultado terá que ser cerca de 50Ω, correspondente à carga existente na outra extremidade do cabo. De notar que com estações activas na rede os valores são diferentes. A tabela 3 lista os vários valores admissíveis numa rede Ethernet.

Resistência	Mín.	Max.
10base2	17Ω	72Ω
10base5	17Ω	72Ω
10baseT	16Ω/100ft	30Ω
Tensão		
10base2	-0.7V	0.7V
10base5	-0.7V	0.7V
10baseT	0V	17V

Tab 3 Valores eléctricos numa rede Ethernet

De notar que durante este tipo de testes a rede tem que estar em algum ponto aberta, pelo que se torna inutilizavel durante as medições.

Os testes possíveis com o multímetro podem ser ampliados com a utilização de um *Time-Domain Reflectometer*, TDR. Para além de curto-circuitos e cortes na cablagem , este equipamento detecta também problemas no isolamento do cabo, dobras e estrangulamentos, o número de estações na rede. O equipamento indica também as distâncias relativas que estas situações se encontram.

Para além destes equipamentos os *leds* indicadores dos vários equipamentos existentes na rede, nomeadamente, *hubs*, *multiport repeaters*, *transceivers*, etc., podem dar uma primeira ideia do que está a acontecer na rede.

Como indicação geral, sempre que seja necessário fazer um diagnóstico devido a uma falha na rede, é fundamental uma abordagem metódica. Antes de avançar para qualquer tipo de acção, deve-se fazer um diagnóstico cuidado do que se passa. Para isso a análise das seguintes condições podem ser uma boa ajuda:

- Se é um problema geral de todos os utilizadores é provável que este se deva a problema físico na rede;
- Se o problema é só de alguns utilizadores então deve ser um problema de configuração local do equipamento que usam;
- Se um computador acede à rede com um pacote de *software* mas não com outro, então o problema é definitivamente de configuração de *software* desse pacote;
- Se por outro lado esse computador não acede à rede com nenhum pacote e outros computadores acedem, então o problema é de *hardware* do computador e deve ser de configuração da sua placa de rede;

Se se chegar à conclusão de que problema é físico, deve-se começar por analisar segmento a segmento, a fim de confinar o problema. Depois do segmento com problemas estar isolado proceder-se-à análise individual da conexão de cada equipamento.

2.3 Ligação à rede

A partir do momento em que as cablagens existem, podem ser os equipamentos ligados à rede. Vamos exemplificar usando PCs.

A primeira questão que se põe é: que placas de rede escolher? Em primeiro lugar, visto estarmos perante uma rede Ethernet, devemos escolher placas Ethernet. Em segundo lugar devem ser escolhidas placas que sejam suportadas pelo barramento da máquina. Por exemplo não poderia escolher uma placa PCI se o barramento da máquina é EISA. Um terceiro aspecto a considerar é o tipo de conector que a placa de rede deve ter. Como já vimos podemos ter redes 10Base2, 10Base5 ou 10BaseT, pelo que serão exigíveis respectivamente conectores BNC, AUI ou RJ45. Existem placas com os três conectores, tal como mostra a fig. 16, embora o mais comum sejam placas com BNC e RJ45. Há no entanto placas mais baratas que só suportam um conector.

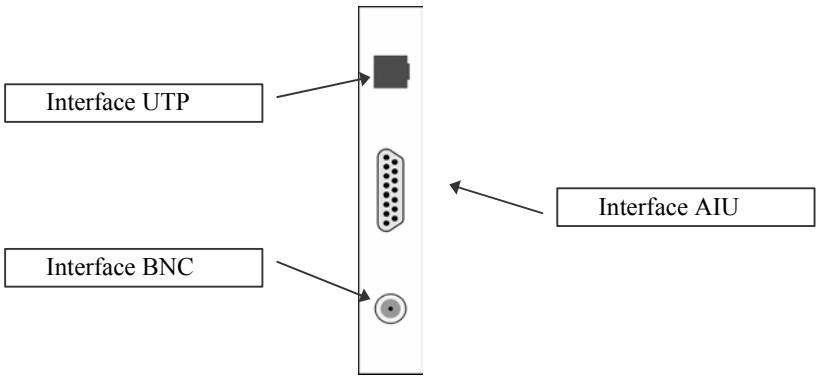


Fig 16 Interfaces de uma placa de rede

As placas de rede têm duas formas de configuração, por *hardware* e por *software*. As primeiras devem ser configuradas antes de serem inseridas nos computadores, sendo esta configuração feita através de *jumpers* e/ou *switches*. No segundo caso, deve ser instalada a placa pois a configuração é feita através de *software* fornecido pelo fabricante.

Os parâmetros básicos que é necessário configurar numa placa de rede, tal como em qualquer outro *hardware* que se insira num PC, são o I/O Address e o IRQ;

2.3.1 I/O Address

O processador precisa de endereçar a memória do computador para trocar informação. Tem também necessidade de ter um espaço de endereçamento para os vários dispositivos. Por

exemplo, o endereço da COM1 é 0x3f8 e o da COM2 é 0x2f8. Também para a placa de rede é necessário definir o endereço pelo qual esta vai responder. Valores típicos são 0x300, 0x320, etc.

2.3.2 IRQ

A forma que o *hardware* usa para avisar o PC de que requer atenção é através de interrupções. Existem interrupções para o disco, para a porta série, etc. Tem também, dentro da gama ainda não usada, escolher um vector de interrupção para a placa de rede. Valores típicos são: 3, 5, 10, 11, etc.

2.3.3 Outros parâmetros

Em alguns casos é ainda necessário configurar outros parâmetros:

- Remote boot: Algumas placas vêm dotadas de uma ROM que permite fazer o *boot* remoto. Quando essa ROM existe é necessário definir o seu endereço. A memória deverá, no caso do MS-DOS ser mapeada na zona entre os 640k e 1024K. Valores típicos a usar são C000h, D000h ou D800h. De referir que alguns controladores de vídeo mapeiam a sua memória a partir de C000h, pelo que dever ser tomado algum cuidado para não atribuir posições já usadas;
- Base memory address: Algumas placas possuem memória que tem que ser mapeada no espaço de endereçamento da memória do computador, também entre os 640Kb e 1024Kb;
- DMA: *Direct memory Access*, é uma técnica de mover dados dentro da memória, sem a necessidade de intervenção do CPU, permitindo assim melhorar o desempenho deste. Algumas placas estão dotadas com esta facilidade, pelo que deve ser configurado o canal DMA a usar;

Nas placas com mais do que um conector é também necessário, nas que não o fazem automaticamente, definir o conector que se vai usar. Em alguns tipos de placas pode-se ainda dizer se a placa é ou não auto-terminada, eliminando a necessidade do T e terminador, ou ainda se se pretende usar cablagens longas não *standard*, permitindo assim que o segmento cresça até 300 m.

Neste momento a instalação física da rede está feita. Agora é tudo uma questão de *software*.

2.4 Equipamentos de interligação

Geralmente uma rede é formada por vários segmentos e por ligações a pontos remotos. A figura 17 apresenta uma instalação típica com vários equipamentos de rede e tecnologias.

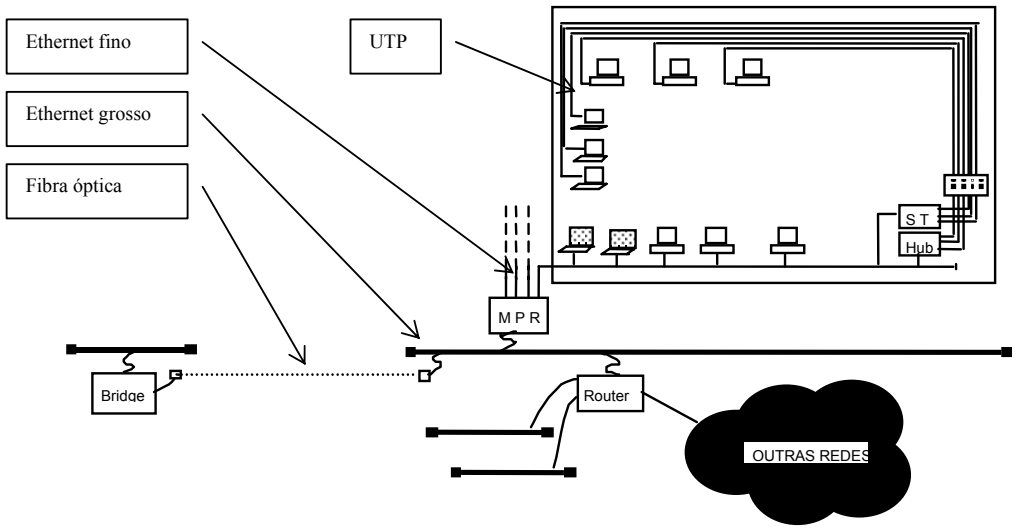


Fig 17 Exemplo de uma instalação

Analisando a rede:

- Esta rede é constituída por um *backbone* em cabo Ethernet grosso, existindo segmentos de cabo fino tirados a partir de um MPR, ***Multiport Repeater***. Este equipamento é um repetidor Ethernet com a particularidade de ter várias portas. Tipicamente têm uma porta AUI e várias BNC visto serem muito usados para a partir de um *backbone* tirar segmentos de cabo fino. Genericamente, um repetidor não trata a informação que circula na rede, apenas reproduz o que recebe, incluindo colisões. É um dispositivo completamente passivo;
- Na sala onde anda o cabo fino existem computadores e terminais X directamente ligados no cabo. Um terminal X é um terminal gráfico com capacidades de rede;
- Existe também um sistema de cablagem estruturada que vai dar a um painel de distribuição, idêntico ao apresentado na figura 15, de onde, conforme a necessidade, se faz a ligação, através de um "chicote", a um ***hub*** ou a um **servidor de terminais**. Um *hub* não passa de um MPR para cabo UTP. O servidor de terminais é um equipamento activo que implementa por exemplo o protocolo *telnet* e ao qual estão ligados terminais, permitindo assim fazer uma ligação de terminal remoto a qualquer sistema, UNIX por exemplo, que esteja na rede. A cablagem estruturada que sai do painel de distribuição segue por uma calha rente ao chão existindo espaçadamente tomadas de ligação onde se poderão ligar computadores, terminais, impressoras, fax, telefones, etc., dependendo apenas das ligações que se fizerem no painel de distribuição;
- Nesta instalação existe ainda um segmento remoto separado por fibra óptica do resto do *backbone*. Ligado a esse segmento existe uma ***bridge***. A *bridge* é um equipamento activo que filtra o tráfego da rede fazendo com que pacotes destinados a máquinas dentro do mesmo segmento não sejam propagados pelo resto do *backbone*, filtrando também as colisões e os pacotes com erros. É, no entanto, completamente transparente para as outras máquinas da rede;
- Finalmente existe um ***router***, encaminhador, que permite a ligação desta instalação a outras redes. Este equipamento é conhecido pelas outras máquinas da rede local. Tipicamente, as máquinas trocam as mensagens directamente entre si quando estão na mesma rede física, enviando os pacotes para o *router* se a máquina destino se encontrar fisicamente separada. Para cada protocolo de nível 3 existe um *router*, embora possam estar todos fisicamente na mesma máquina. Exemplos de protocolos que necessitam de encaminhamento são: IP da pilha Internet, IPX da Netware, XNS da Xerox, Appletalk da Apple, etc;

- Não representado na figura, mas com uma utilização cada vez maior são os ***switches***. Estes equipamentos não são mais do que a mistura de *hubs* com *bridges*. Resulta assim um *hub* em que uma porta só recebe tráfego se o computador destino da informação estiver ligado a essa porta, contrariamente aos *hubs* tradicionais que quando recebem um pacote o retransmitem para todas as portas. Desta forma há um muito melhor aproveitamento da largura de banda disponível em cada porta pois não está a ser ocupada por tráfego desnecessário. No entanto estes equipamentos não filtram *broadcasts*, pacotes que são enviados para todas as máquinas de uma rede. Para isso e porque, como veremos mais adiante, nem todas as mensagens de *broadcast* interessam a todos os elementos da rede, surgiram equipamentos ainda mais sofisticados, os chamados ***switches* de nível 3**, que são *switches* que incorporam funcionalidades de encaminhamento.

2.5 A evolução do Ethernet

As exigências sobre as redes são cada vez maiores, pelo que são necessárias redes mais rápidas. Para responder a estas exigências, também o Ethernet evoluiu para o Fast Ethernet e para o Giga Ethernet

2.5.1 Fast Ethernet

Esta norma, definida pelo IEEE sob o nome de IEEE 802.3u e também conhecida por 100Base-T, designa um tipo de rede Ethernet que funciona a 100Mbps. Neste momento é a tecnologia mais usada a seguir ao Ethernet e é o caminho mais natural para a sua evolução. Isto porque o princípio de funcionamento é o mesmo e muitas das placas de rede hoje em dia no mercado permitem as duas velocidades de transmissão. Além disso são muito vulgares os *hubs* e *switches* 10/100Mbps.

Em termos de infra-estrutura física o Fast Ethernet fornece três sistema de cablagem distintos:

- 100Base-TX. Usa dois pares, um para transmitir outro para receber, de um cabo de par trançado de alta qualidade tail como o UTP cat. 5 ou IBM Type 1 STP. A distância máxima permitida é de 100m entre um *hub* e um nó. A vantagem este sistema é que suporta a transmissão *full-duplex*. A desvantagem é que obriaga a um tipo de cablagem de melhor qualidade, bem como conectores e outros elementos;
- 100Base-T4. Usa quatro pares, um para enviar, outro para transmitir e os restantes bi-direccionais, de um cabo de par trançado de qualidade média, tal como o UTP cat. 3. Na prática o que se faz é dividir o sinal por três pares de forma a que a taxa de transmissão se mantém mas a uma frequência do cabo muito mais baixa. A distância máxima permitida é de 100m entre um *hub* e um nó. A vantagem deste sistema é que funciona virtulamente com qualquer tipo de cablagem UTP existente. As desvantagens são de que requer quatro pares trançados e não suporta *full-duplex*;
- 100Base-FX. Especifica o mesmo tipo de cablagem de fibra óptica usada pelo 10BaseFL. A distância máxima é de 185m entre um *hub* e um nó. No caso de uma ligação *full-duplex* a distância pode ir até 2000m. A especificação física da fibra são as mesmas do 10BaseFL embora sejam preferidos conectores do tipo SC. As vantagens são as habituais na fibra óptica: maiores distâncias, imunidade electromagnética e maior segurança. A maior desvantagem desta tecnologia ainda é o preço.

Uma das vantagens da utilização de um sistema de cablagem estruturada baseada em par trançado é de que "basta" trocar as placas dos equipamentos e os *hubs* para que a rede esteja

pronta a funcionar. O único problema, que não é de desprezar, são as instalações de cabo coaxial, que têm que ser substituídas, pois não são suportadas por esta nova tecnologia.

Actualmente é vulgar existirem soluções mistas em que a espinha dorsal da rede é em Fast Ethernet e com *hubs* 10/100, em que este tem uma porta a 100Mbps para ligar ao *backbone* e as outras a 10Mbps para os utilizadores, havendo eventualmente mais uma ou duas portas a 100Mbps para ligar servidores. Nas soluções mais exigentes usa-se apenas o Fast Ethernet. Uma possibilidade de aumentar ainda o desempenho destas redes é a utilização de *full-duplex*, permitido na maioria dos *hubs* e *switches*. Isto é possível pois sendo as ligações em estrela a interligação entre os equipamentos é ponto a ponto e, a transmissão e recepção é feita em canais separados, pelo que não existe o problema do acesso ao meio.

De notar que existe uma outra tecnologia de 100Mbps chamada de 100VG-AnyLAN, formalizada pelo comité 802.12 do IEEE, sob proposta de vários fabricantes liderados pela Hewlett Packard e cujo formato da trama é idêntico ao do Ethernet mas Esta norma não teve tanto sucesso e e por isso conta com muito menor expressão no mercado.

Esta norma usa dois pares de fios de cablagens do tipo UTP cat. 3, em que ambos os pares são utilizados para transmitir e receber, não sendo por isso possível implementar a operação *full-duplex*.

2.5.2 Giga Ethernet

Esta tecnologia é o mais recente avanço em termos da já longa história do Ethernet e está a ser padronizada pelo IEEE através do comité 802.3z. Em termos físicos é utilizada a tecnologia Fiber Channel para a codificação do sinal. Em termos de cablagem existem as seguintes propostas:

- 1000BaseLX (Long Wavelenght). Usa fibra *singlemode* e serve principalmente para interligação de redes que podem ir até 3km;
- 1000BaseSX (Short Wavelenght). Usa fibra *multimode* e serve principalmente para *backbone* de edifícios até 500m;
- 1000BaseCX (Short Haul Copper). Usa cabo coaxial até 25m e serve principalmente paralgação de servidores a *switches* e ligações entre estes;
- 1000BaseT (Long Haul Copper). Usa cabo UTP até 100m e serve principalmente para a ligação de computadores de escritório;

De notar que as duas últimas tecnologias ainda não estão padronizadas.
O modo de operação tanto pode ser *haf-duplex* como *full-duplex*.

2.6 Tecnologias de interligação

Para a interligação de redes locais são usadas outras tecnologias. A título informativo ficam aqui referidas algumas delas.

2.6.1 FDDI

O Fiber Distributed Digital Interface tem sido largamente usado para a criação de *backbones* de grandes redes locais a uma taxa de transmissão de 100Mbps. Baseia-se na norma ANSI X3T9.5 e usa a fibra óptica como meio de transmissão e tendo o Manchester diferencial como método de codificação. A trama tem um tamanho de 4500 *bytes*. O tamanho máximo da rede é de 100km e a distância máxima entre estações é de 2km. O número máximo de estações na rede é de 500.

A rede é formada por um duplo anel onde a informação circula, em cada anel, no sentido inverso uma da outra de modo a que possam formar um anel único no caso de uma falha na rede. As estações funcionam como repetidores e podem estar ligadas aos dois aneis ou apenas ao anel primário. Tipicamente não são computadores que estão directamente ligados ao anel, mas antes equipamento de comunicações tal como *switches* e *routers* dos quais depois sai a infra-estrutura

de rede local.

Existe também uma variante do FDDI que usa cobre ao invés de fibra, designando-se por CDDI.

2.6.2 ATM

O Asyncronous Transfer Mode é uma tecnologia que tanto pode ser usada para redes locais de computadores, LANs, como também para grandes redes, WANs. Actualmente é a tecnologia mais promissora em termos de integrar o mundo das redes de dados com as redes de telecomunicações. Isto porque integra a noção de qualidade de serviço. Neste contexto a qualidade de serviço tem a ver com a largura de banda a disponibilizar para o serviço ser prestado com qualidade. Por exemplo uma emissão vídeo não pode ser transmitida com a mesma largura de banda que que a voz num telefonema pois a qualidade da transmissão seria inaceitável. Assim, quando uma aplicação solicita os serviços da rede deverá especificar a qualidade de serviço pretendida em função do tipo de informação a transmitir. Por essa razão o ATM suporta vários tipos de tráfego, tal como voz, dados, fax, vídeo em tempo real, áudio com qualidade de CD e imagem.

A largura de banda disponibilizada é de 155Mbps, podendo ir a 622Mbps na interligação entre *switches* e é usado sobre fibra óptica, podendo ser usado UTP na ligação aos computadoes de escritório. Uma rede ATM éconstituída por um conjunto de *switches* interligados entre si, dos quais saem redes locais, ou ligações a outros sistemas de comunicações.

O ATM baseia-se no conceito de comutação de pacotes, aqui chamadas de células. Cada célula tem um tamaho fixo de 53 *bytes*. Os *switches* apenas se encarregam de fazer passar as células, verificando o seu cabeçalho e reencaminhando-as logo de seguida. Como o tamanho destas é fixo, o atraso é mínimo. Toda esta operação de *switching* é feita por hardware e não há verificação de erros pois é assumido que a infra-estrutura de comunicações é de alta qualidade.

2.6.3 Frame Relay

Para estabelecer conexão entre redes locais remotas é necessário recorrer a serviços oferecidos pelos operadores de telecominocações. O FDDI não é tipicamente oferecido por estes operadores pois enquadra-se no âmbito das redes locais. Por outro lado o ATM só agora começa a ser oferecido pelos operadores e a custos elevados. Assim, a tecnologia que melhor se adapta a este tipo de serviços é o Frame Relay. É a tecnologias de grandes redes, WANs, mais utilizada e veio substituir outra equivalente mas com menor desempenho, o X25. O Frame Relay evoluiu a partir do X.25 e do RDIS, oferecendo um serviço orientado ao pacote numa rede de comutação de circuitos com taxas de transferênciade 56Kbps até 1,544Mbps.

O Frame Relay opera no primeiro e segundo nível do modelo de referência OSI, utilizando o LAPD, uma variante do HDLC, como protocolo de nível 2.

2.6.4 RDIS

O RDIS, Rede Digital de Integração de Serviços, ou ISDN, é o equivalente às linhas telefónicas existentes nas nossas casas, com a vantagem de ser digital e não analógica como as linhas tradicionais. O RDIS pode existir em duas versões:

- BRI, Basic Rate Interface. Para pequenas empresas e residências, composto por dois canais de 64Kbps para dados e uma canal de 16Kbps para controlo;
- PRI, Primary Rate Interface. Para grandes empresas e composto por canais de 64kbps, 23 para dados e um para controlo.

O RDIS é uma solução atractiva para quem não tem uma necessidade permanente de acesso remoto mas pretende ter um serviço de qualidade.

Para uma ligação externa permanente, o Frame Relay é uma solução mais vantajosa.

3 O nível lógico

O objectivo desta camada pegar numa linha fisida de transmissão e torna-la num meio fiável de transmissão de dados.

O nível lógico, do modelo de referência OSI é usualmente subdividido em dois nas redes locais de computadores, tal como mostra a fig. 18.

Assim existe a sub-camada MAC, *Medium Access Control*, e a sub-camada LLC, *Logical Link Control*. O primeiro, mais perto do nível físico, cuida de pôr e tirar a informação nos cabos. O segundo cuida da ligação entre dois dispositivos de rede, nomeadamente, tipo de serviço de comunicação, controlo de fluxo, correcção de erros, etc.

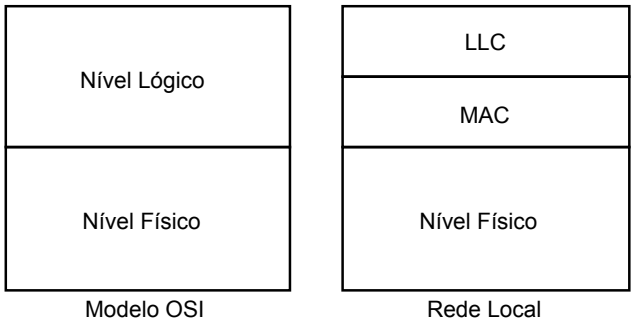


Fig 18 O modelo de referência aplicado a uma rede local

Um dos protocolos de nível 2 mais usados é o HDLC, *High-Level Data Link Control*. O LLC não é mais do que uma implementação de um subconjunto do HDLC aplicado às redes locais. No entanto este protocolo não é suficiente pois nas redes locais geralmente o meio de transmissão é partilhado. Isto implica que tenha que existir "alguém" que faça a gestão do acesso ao meio. Daí a necessidade de subdividir o nível 2, e a necessidade de aparecer o sub-nível MAC.

A norma Ethernet, tal como indica a fig. 19, apenas implementa a sub-camada MAC do nível lógico. As funções do LLC passam a ser implementadas pelos níveis superiores, excepto a detecção de erros que é feita pelo MAC.

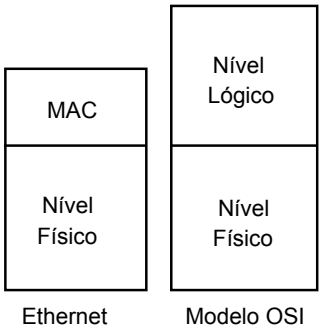


Fig 19 A implementação do Ethernet

Tal como já foi referido no início deste texto, o IEEE, normalizou alguns protocolos para redes locais de computadores.

Temos assim, tal como mostra a fig. 20, foram definidos 3 protocolos do nível físico e MAC:

- IEEE 802.3, define uma rede em barramento com o CSMA/CD como forma de acesso ao meio. Esta norma é muito parecida com o Ethernet;
- IEEE 802.4, define uma rede em anel com o *Token-ring* como forma de acesso ao meio;

- IEEE 802.5, define uma rede em barramento com o *Token-bus* como forma de acesso ao meio;

Como protocolo da sub-camada LLC é definido o IEEE 802.2.

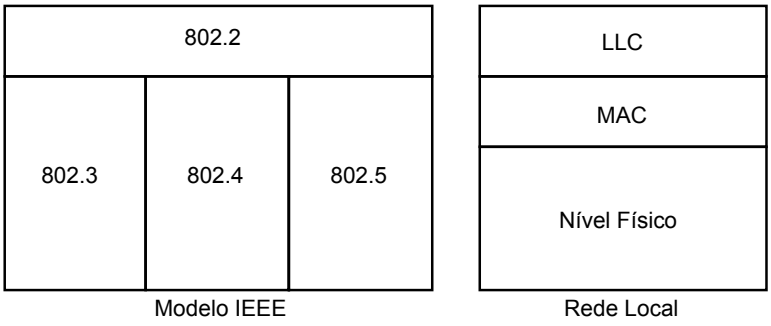


Fig 20 A implementação IEEE

3.1 A sub-camada MAC

Não devemos ficar com a ideia que o protocolo Ethernet apenas define as especificações dos cabos a usar, os seus comprimentos máximos e a forma como electricamente os *bits* são codificados. O protocolo Ethernet vai muito mais além. Define por exemplo o formato da informação que circula na rede e o método de acesso à rede.

3.1.1 O formato da informação

O Ethernet não transmite para a rede uma sequência aleatória de *bits*, mas antes uma trama estruturada, tal como se pode ver pela figura 21.

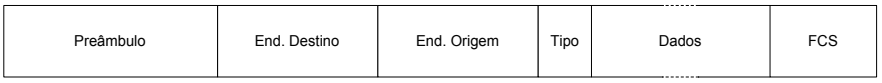


Fig 21 Formato da trama Ethernet

Importa antes do mais referir que neste momento existem duas normas relativas ao Ethernet. A norma Ethernet propriamente dita, a Ethernet II, e uma norma IEEE, o IEEE802.3.

Estas normas são muito parecidas, sendo a grande diferença a função atribuída ao quarto campo da trama. Digamos assim que a diferença é de *software* e não de *hardware*, pelo que todas as placas de rede podem enviar e/ou receber qualquer dos dois tipos de trama. Isto não quer dizer que as estações de rede enviem indiscriminadamente tramas de um e de outro tipo. O que acontece é que há protocolos que usam um tipo de trama e outros que usam outro. Isto é, um computador pode estar a falar simultaneamente com um que "fala" Ethernet e outro que "fala" 802.3. Por exemplo, TCP/IP e DECNET falam EthernetII. Por outro lado SNA e NetBIOS falam 802.3. O Netware é configurável entre as duas opções.

Vamos então analisar os vários campos de uma trama Ethernet/802.3:

- Preâmbulo: 8 *bytes*. O preâmbulo é usado para que a máquina destino possa sincronizar e receber a trama correctamente. É constituído por uma sequência de 1s e 0s, com a excepção do último bit que é também 1 pois serve para indicar que a partir daí começa o endereço destino da trama. Por curiosidade, o último octeto, onde se encontra a excepção à sequência de 1s e 0s, é chamado pela norma 802.3 de Start Frame Delimiter, delimitador de início de trama;

- Endereço Destino/Endereço Origem: 6 *bytes*. Quando uma estação pretende comunicar com outra, tem que ter uma forma de a endereçar. Estes endereços são constituídos por 6 *bytes*. Este endereço já vem na própria placa. Antes do endereço destino são enviados 8 octetos com bits 0 e 1 alternadamente, para sincronização, o preâmbulo, estando a 1 os últimos dois bits desta sequência;
- Tipo/Tamanho: 2 *bytes*. Este é o campo da discórdia. No Ethernet representa o tipo da informação contida na parte de dados da trama. Imagine que a trama é um camião de carga. Este campo indica o tipo de carga que o camião leva. A tabela 4 indica vários exemplos para este campo.

Tipo	Protocolo
0x0600	XNS
0x0800	IP
0x0806	ARP
0x6006	DECNET

Tab 4 Exemplos para o campo *type* da trama Ethernet

No 802.3 este campo representa o tamanho do campo dados.
A forma de distinguir uma trama Ethernet de outra 802.3 é a seguinte: se este campo tiver um valor decimal inferior a 1500, a trama é 802.3, senão é uma trama Ethernet.

- Dados: 46 a 1500 *bytes*. A informação transportada na trama.
- CRC: 4 *bytes*. Controlo de erros da trama.

Como já foi dito, e por comparação, uma trama Ethernet é um camião em que a caixa de carga é o campo dados e, a origem, o destino e o tipo/quantidade de carga transportada, fazem parte da guia de transporte que o motorista leva.

3.1.2 O acesso ao meio

Sendo a rede Ethernet do tipo barramento em que todas as estações podem ter acesso ao meio e sabendo também que em cada instante apenas uma pode usar o meio, como fazer a gestão dos acessos?

Imaginemos uma pista em que só cabe um carro, figura 22. Como é que esse carro vai de uma garagem para a outra?

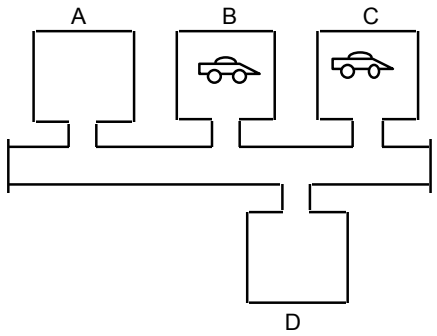


Fig 22 O meio está livre

O que o condutor dever fazer é ver se está alguém a circular na pista. Se a pista estiver vazia avança. Fig. 23.

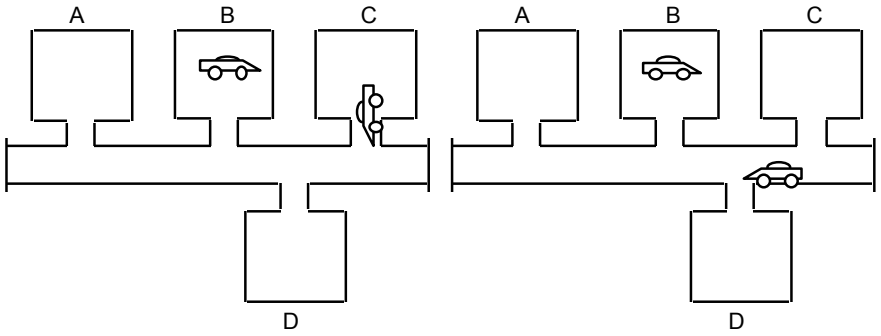


Fig 23 Escuta e acesso ao meio

Se um condutor pretender sair enquanto outro se encontra na pista, o que tem a fazer é esperar. Fig. 24.

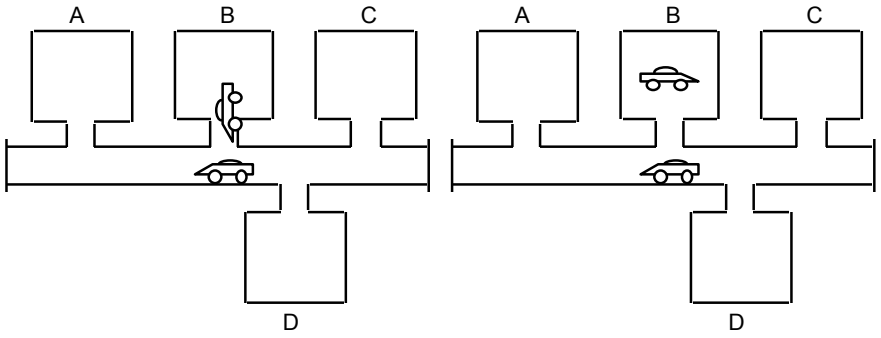


Fig 24 O meio está ocupado

No entanto, pode dar-se o caso de que ambos os condutores pretendem sair e ambos detectam o meio livre. neste caso a colisão será inevitável, fig. 25. O melhor a fazer é voltar para casa e tentar mais tarde.

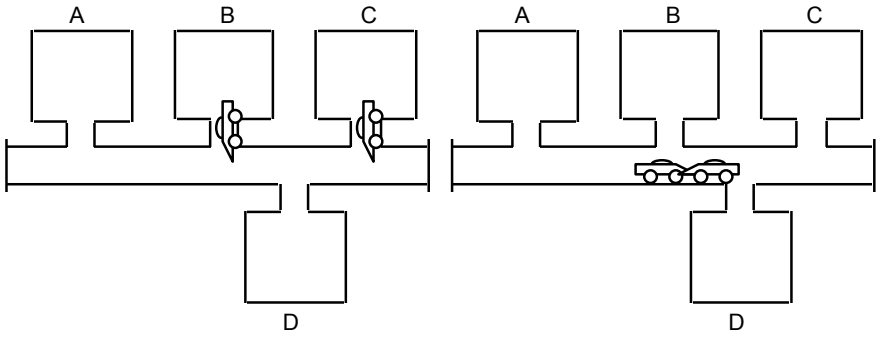


Fig 25 A colisão é inevitável

O método usado pelo Ethernet para aceder ao meio é o CSMA/CD, *Carrier Sense Multiple Access with Collision Detection*, e o paralelismo com o exemplo anterior é total. Assim, antes de ser enviada qualquer coisa para a rede o meio é escutado para ver se este está livre. Caso isso não aconteça, o meio é monitorizado até estar livre. A partir desse instante é iniciada a transmissão.

Se o meio estiver livre é iniciada a transmissão, estando a estação a escutar ao mesmo tempo o meio para ver se o que aí circula é o que foi enviado. Desta forma está a ser escutado o meio para detectar eventuais colisões fruto de transmissões simultâneas. No caso de ser detectada uma colisão, é lançado no meio um sinal de erro e todas as estações param de transmitir. Uma nova

tentativa de transmissão vai ser atrasada, não um valor constante, mas um valor aleatório obtido através de um algoritmo de retirada exponencial, isto é, o tempo de espera vai aumenta à medida que as tentativas de transmissão seguintes geram colisões. Esta versão do CSMA/CD é chamada de 1-persistente e é a que é usada no Ethernet/802.3. Existem outras versões, nomeadamente, não persistente, em que quando a estação que quer transmitir detecta o meio ocupado utiliza o algoritmo de retirada exponencial. Se o meio estiver livre, inicia a comunicação. Outra variante é a p-persistente, em que escuta o meio até este estar livre, mas existe uma probabilidade p de iniciar a transmissão.

3.2 A sub-camada LLC

Como já foi referido o Ethernet não implementa directamente esta sub-camada. Geralmente, dentro da trama do sub-nível MAC segue um pacote do nível de rede. O campo Tipo, da trama, identifica o tipo de informação contida. Por exemplo, no caso do TCP/IP, dentro do campo DADOS da trama Ethernet segue um pacote IP, indo no campo TIPO o valor 0x800.

O IEEE define uma norma para o LLC, para ser usada sobre a camada física+MAC. Esta norma é o IEEE 802.2. Esta norma define os serviços fornecidos, a especificação do protocolo e o *interface* com o sub-nível MAC.

A tabela 5 define os três tipos de serviços organizados em quatro classes, fornecidos pelo LLC.

		Classes LLC			
		I	II	III	IV
Tipos de operações suportadas	1	•	•	•	•
	2		•		•
	3			•	•

Tab 5 Tipos de operação suportadas pelo LLC e respectivas classes

O tipo 1 implementa um serviço não orientado à conexão sem *acknowledgment*. É um serviço não fiável e não orientado à conexão, isto é, a trama é enviada e esquecida. Não é estabelecida nenhuma conexão entre os dispositivos que estão a comunicar e também não é dada nenhuma informação por parte do destino sobre a chegada da trama.

O tipo 2 implementa um serviço orientado à conexão. É estabelecida uma conexão antes de se proceder à troca de informação. Além disso, a troca de dados é acusada pelo destinatário, garantindo que os dados chegaram correctamente. Para obter um maior aproveitamento do meio físico, usa um conceito de janela deslizante adaptativa, que será visto mais à frente, permitindo assim o balanceamento da carga da informação que circula na rede.

O tipo 3 implementa um serviço não orientado à conexão com *acknowledgment*. É um misto dos tipos anteriores, em que é feita a acusação correcta dos dados, por parte do destino, sem no entanto ser estabelecida qualquer conexão.

Dentro da trama 802.3 segue a trama 802.2, que implementa os serviços acima indicados.

Por comparação com os serviços oferecidos pelo IEEE 802.2, podemos dizer que o Ethernet implicitamente implementa o serviço do tipo 1, sem no entanto ser inserida uma trama LLC na trama MAC.

4 Os drivers*.*

Para que as placas de rede funcionem necessitam de algum *software* de baixo nível que inicialize a placa, execute as funções necessárias para interagir com os protocolos de níveis

superiores, gira os *buffers*, etc. O *software* responsável por estas tarefas é o *driver* da placa.

No ambiente dos PCs, o sistema operativo não tem a capacidade por si só de comunicar com a placa de rede. Por isso é necessária a existência de "qualquer coisa" que comunique com a placa de rede, o *driver*. Se esta "peça" não existisse, os produtos lógicos de comunicações teriam que ser feitos à medida da placa de rede, isto é, teria que existir uma versão do *software* para cada uma das placas existentes no mercado, ou pelo menos para as mais vulgares. Por outro lado isto implicaria que cada aplicação tomasse como sua a placa de rede, não podendo assim ser partilhada por vários protocolos/aplicações.

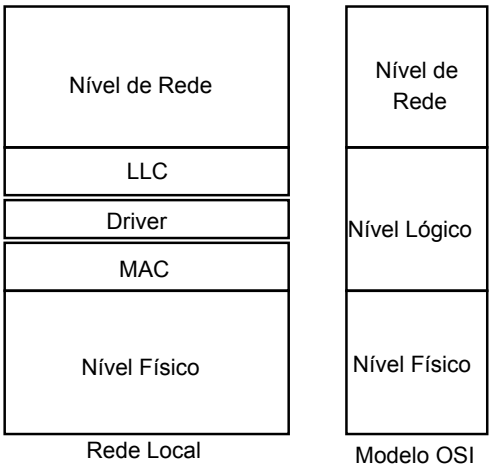


Fig 26 O driver da placa de rede e o modelo OSI

Esta arquitectura não se nota muitas vezes nos sistemas UNIX pois estes geralmente contêm o *driver* para o *hardware* Ethernet, integrado no sistema operativo pelo que não é necessário fazer nada para que tudo funcione correctamente.

Vamos ver o papel do *driver*. Normalmente, a placa de rede faz uma filtragem dos pacotes recebidos, aceitando apenas aqueles que não têm erros e cujo endereço destino seja o seu, ou então o endereço de *broadcast*. Todos os pacotes que superam este filtro são passados ao *driver*, através de um *interrupt* de *hardware*. O *driver* é *software*, pelo que o processamento que ele faça aos pacotes vai requerer tempo de CPU. A sua tarefa será passar os pacotes, da placa de rede para a memória do computador, passando-os depois aos protocolos de nível superior.

Existem actualmente no mercado três tipos de *drivers* que fazem este papel e que geralmente acompanham as placas de rede para PC:

- Packet Drivers. Criados a partir da especificação feita pela empresa FTP Software. Usado por vários pacotes de *software*, incluindo NCSA Telnet e as aplicações da FTP Software;
- NDIS. *Network Driver Interface Specification*. Desenvolvido por Microsoft e 3Com; Usado por Lan Manager, Windows for Workgroups, Windows NT;
- ODI. *Open Datalink Interface*. Desenvolvido por Novell e Apple. Usado pelo NetWare.

5 O nível de rede

Esta camada é responsável pelo encaminhamento da informação desde a origem até ao destino.

Um *software* que esteja desenhado apenas para uma rede local não necessita deste nível. Um exemplo deste tipo é o *software* que suporta o ambiente de rede no Windows for Workgroups e Windows 95, o NetBEUI, NetBIOS *Extended User Interface*.

O objectivo fundamental do nível 3 da pilha OSI é permitir *internetworking*. Isto é, permitir a comunicação entre todos os sistemas pertencentes redes que estão interligadas entre si. Dito de outra forma, faz o encaminhamento da informação.

Como analogia tomemos o seguinte exemplo:

> "O João pretende ir de Braga ao Algarve. Para isso dirige-se à central de camionagem e pergunta qual o autocarro para o Algarve. O funcionário responde que não existe um autocarro directo, mas que deve tomar o autocarro para o Porto. Chegado ao Porto o João faz a mesma pergunta, tendo-lhe sido respondido que devia tomar o autocarro em direcção a Lisboa. Aí chegado, mais uma vez foi ter com as informações da central e aí, indicaram-lhe, (finalmente!!!) que havia uma autocarro para o Algarve."

Um protocolo de nível 3 faz exactamente isto, leva a informação desde a origem até ao destino, tendo a capacidade de, no emaranhado de destinos possíveis saber os que lhe interessam.

5.1 O protocolo IP

O protocolo de nível de rede mais usado é o IP, Internet Protocol.

Este protocolo, em conjunto com outros protocolos de nível superior formam a infraestrutura da Internet. A figura 27 apresenta o enquadramento do conjunto destes protocolos no modelo OSI.

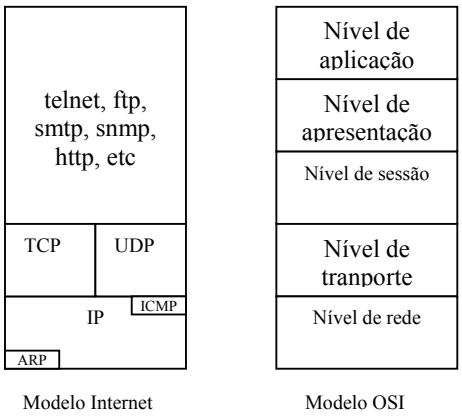


Fig 27 Os protocolos TCP/IP no modelo OSI

O IP é um protocolo que oferece um serviço não fiável e não orientado à conexão onde a funcionalidade de encaminhamento é intrínseca ao tipo de endereço usado. Como se pode ver pela figura 28, cada rede tem um endereço e, dentro de cada rede, cada máquina tem também um endereço. Assim, podemos dizer que o endereço A.b corresponde à maquina b que se encontra na rede A.

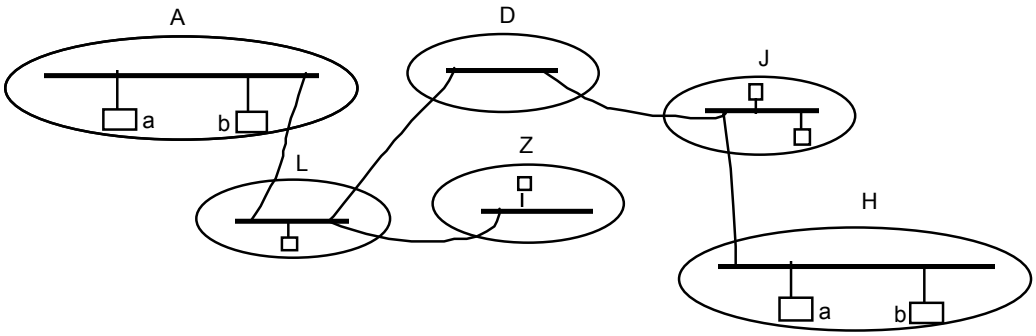


Fig 28 Uma *internet*

Com base nesta filosofia os endereços IP são endereços formados por quatro octetos, sendo parte para endereçar a rede e parte para endereçar a máquina.

Um endereço IP tipicamente tem o seguinte formato A.B.C.D, em que A,B C e D representam valores numéricos de 8 bits.

Por exemplo 193.136.14.253 e 12.123.123.123 representam endereços IP.

5.1.1 As classes de endereços

Dentro do endereço IP são estabelecidas 3 classes de endereços, classe A, B e C.

A classe A define 1 octeto para redes e 3 para máquinas. Os endereços de 1.X.X.X a 126.X.X.X representam endereços de classe A. Existem assim 126 redes desta classe com a hipótese de um número gigantesco de máquinas para cada rede.

A classe B define 2 octetos para redes e dois para máquinas, permitindo endereços desde 128.1.X.X até 191.254.X.X. De referir que o endereço 127.X.X.X está reservado para *loopback*.

A classe C define 3 octetos para redes e 1 para máquinas, permitindo endereços desde 192.1.1.X até 223.254.254.X. Os endereços acima de 223 estão reservados, para a classe D, *multicast*, e classe E.

Esta divisão em classes serve para facilitar o encaminhamento da informação e, como que representa três tipos de organizações, grandes médias e pequenas.

Imagine-se uma grande organização. Se lhe for atribuído um endereço de classe A, para quem está fora só existe uma rede, podendo todo o encaminhamento ser feito para aí. No caso de serem atribuídos dezenas de endereços de classe C, quem está fora teria que ter todas essas redes nas suas tabelas de encaminhamento. Daí o interesse de dividir o espaço de endereçamento em classes.

5.1.2 Sub-endereçamento

Como vimos, um endereço de classe A pode endereçar uma quantidade brutal de máquinas. Na prática não é isso que acontece. O que se passa é que esse espaço gigante é dividido em sub-redes, tendo cada sub-rede o espaço para as suas máquinas.

Esta noção de sub-redes é feita à custa de uma máscara, a máscara de rede. Tomemos como exemplo um endereço de classe B. Por defeito um endereço de classe B, tem a máscara de rede 255.255.0.0, ou em binário, 11111111.11111111.00000000.00000000. Isto é, 2 octetos definem a rede como é típico de um endereço de classe B.

No entanto, pode-se dentro de uma rede de classe B, por exemplo querer usar o terceiro octeto para definir sub-redes, obtendo desta forma 254 sub-redes. A máscara de rede passaria a ser 255.255.255.0. Teríamos assim uma rede classe B com 254 sub-redes, em que cada uma poderá ter 254 máquinas.

Por exemplo para a rede 191.2.0.0, se se usar a máscara 255.255.0.0, os endereços 191.2.3.4 e 191.2.4.5, representam a máquina 3.4 e 4.5 respectivamente, da rede 191.2. Por outro lado se a mesma rede usar a máscara 255.255.255.0, os mesmos endereços já representam a máquina 4 da sub-rede 3 e, a máquina 5 da sub-rede 4 respectivamente, da mesma rede. Desta forma na rede

191.2 podem existir as sub-redes 191.2.1.X até 191.2.254.X, como possibilidade para 254 máquinas em cada uma.

O significado de 0 e 255

Nos exemplos referidos até aqui não foi usado nem 0 nem 255 nos endereços IP. Estes valores têm um significado especial num endereço de rede. O valor 0 na identificação da máquina significa a rede e é o endereço usado em casos particulares, quando uma máquina não sabe o seu endereço na rede. O valor 255 representa um endereço de difusão, *broadcast*. Quando uma máquina deseja enviar uma mensagem a todas a que estão na rede usa o endereço da sua rede com tudo a 1 na parte da máquina. por exemplo o endereço 193.136.14.255 é o endereço de difusão da rede 193.136.14.

5.1.3 O formato do datagrama IP

Um datagrama IP, figura 29, é formado por um cabeçalho e um campo de dados, onde seguem os protocolos de nível de transporte.

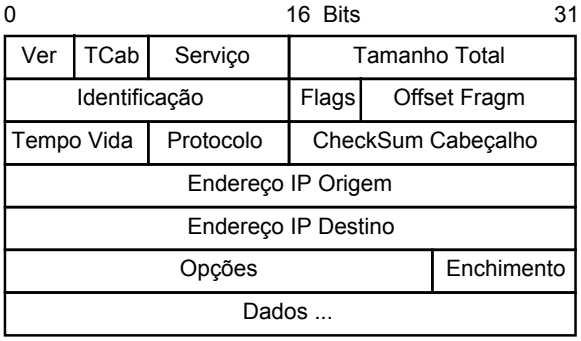


Fig 29 O datagrama IP

O cabeçalho é formado, para além de alguns campos adicionais, por um endereço IP origem e um endereço IP destino, isto é um remetente e um destinatário da informação.

Dos campos adicionais do cabeçalho, de realçar os campos Identificação, Flags e Offset Fragm, pois permitem a implementação do conceito de fragmentação.

Os outros campos são:

- Ver: Versão do protocolo;
- TCab: Tamanho do cabeçalho, medido em palavras de 32 bits;
- Serviço: determina a qualidade de serviço pretendida pelo datagrama;
- Tamanho Total: Tamanho total do datagrama;
- Tempo Vida: Especifica o tempo de vida de um datagrama. Sempre que um datagrama passa num *gateway* o seu tempo de vida é decrementado. A ideia é evitar que um datagrama ande em ciclo na rede;
- Protocolo: Este campo é idêntico ao campo Type da trama Ethernet. Indica qual o protocolo que segue no campo dados;
- Checksum Cabeçalho: permite testar a integridade do cabeçalho IP;
- Opções: Este campo é opcional, de tamanho variável e é usado principalmente para teste e *debug*;
- Enchimento: No caso de existir o campo anterior, são-lhe inseridos *bits* a 0 de forma a que a soma dos dois campos atinja os 32 *bits*.

5.1.4 Fragmentação

Pelo campo Tamanho Total podemos ver que um datagrama IP pode ter no máximo 65535 octetos. Para que uma trama Ethernet, por exemplo, pudesse conter um datagrama IP seria

necessário que o seu campo de dados pudesse ter um tamanho igual ao do datagrama. Acontece que o Ethernet define como tamanho máximo da trama 1514 octetos, sendo no máximo 1500 para dados. Desta forma, ou o datagrama IP não ultrapassa 1500 octetos, ou então o protocolo implementa um mecanismo de fragmentação e reagrupamento do datagrama. A primeira solução não é viável pois para cada meio físico existe um MTU, *Maximum Transfer Unit*, diferente. Desta forma, por exemplo, quando um datagrama viaja por uma *internet*, e se depara com troços que suportam menores MTU, não se poderia adaptar e não poderia passar por esses troços. Assim, a segunda solução é a mais modular, que permite a utilização do IP sobre qualquer meio físico.

5.1.5 Encaminhamento

Como já foi referido, o papel do IP é procurar as rotas necessárias para que um datagrama chegue à máquina destino.

Temos no entanto que separar duas situações:

- A maquina destino está na mesma rede IP;
- A máquina destino está noutra rede IP.

Um exemplo do primeiro caso temos a comunicação entre as máquinas A e B, da figura 30. Quando um datagrama chega ao nível IP, vinda dos níveis superiores, a fim de ser transmitida o IP vai analisar a parte da rede do endereço IP, chegando à conclusão de que a máquina destino de encontra na mesma rede IP. Neste caso o IP vai inserir o datagrama numa trama Ethernet, endereçada a B. Embora ainda não tenha sido referido, neste momento já deve ser claro que o IP e o Ethernet usam um esquema de endereçamento diferente. O mapeamento entre os dois é feito através do ARP, *Adress Resolution Protocol*.

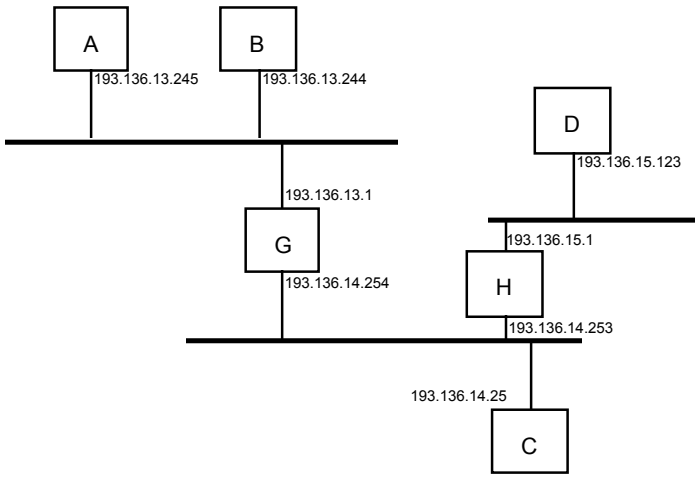


Fig 30 *Gateways* numa rede IP

O segundo caso é o exemplo típico para o qual o IP foi criado. Como exemplo tomemos a comunicação entre as máquinas A e C, da figura 30. Neste caso o IP vai detectar que a máquina destino se encontra noutra rede IP. O datagrama IP, que tem como endereço origem a máquina A e como endereço destino a máquina B, será no entanto inserido numa trama Ethernet endereçada à máquina G, o *gateway*. O que acontece é que quando no IP uma máquina endereça outra que não está na mesma rede, a máquina origem passa o datagrama IP a um *gateway* a fim de que este o encaminhe. O *gateway* G quando recebe a trama Ethernet desempacota o datagrama IP e vai analisar o seu endereço destino. Através da consulta da sua tabela de encaminhamento G detecta que tem um *interface* na mesma rede que C. G então insere o datagrama original numa trama Ethernet endereçada a C.

Um caso um pouco mais complexo é a comunicação entre A e D. Neste caso, quando o *gateway* G recebe o datagrama de A, verifica que não está directamente ligado à rede onde D se encontra. No entanto D tem na tabela de encaminhamento a indicação de que os datagramas para a rede 193.136.15.0 deverão ser endereçados ao *gateway* H. Então G altera dois campos do cabeçalho IP, decrementando o campo Tempo Vida e calculando um novo valor para o campo Checksum Cabeçalho, insere o datagrama numa trama Ethernet e endereça-a a H. Este recebe então a trama, retira o datagrama IP e como está na mesma rede de D envia-lhe directamente o datagrama.

Por estes exemplos retirar várias conclusões:

- Todo o conceito de encaminhamento está baseado na parte da rede do endereço IP;
- Por muitos *gateways* que passe, os endereços origem e destino do datagrama IP nunca são alterados;
- O encaminhamento é feito pelos *gateways* à custa das consultas das suas tabelas de encaminhamento.

A grande dificuldade em todo este processo é a criação e manutenção destas tabelas de encaminhamento. Esta tarefa não é da responsabilidade do IP mas sim dos protocolos de encaminhamento implementados pelos *gateways*.

5.2 O protocolo ARP

Na secção anterior é usada várias vezes uma frase do género: "A máquina A insere o datagrama IP numa trama Ethernet e endereça-a a B."

Até agora ainda não tinha sido abordada a questão de como é que um datagrama IP chega à máquina destino. Sabemos que essa comunicação tem que ser pelo Ethernet, ou outro qualquer protocolo físico. Sabemos também que o nível físico usa um tipo de endereçamento que é incompatível com o IP.

A conclusão a que se chega é de que tem que haver alguém que se encarregue de estabelecer a relação entre endereço IP e endereço físico. Esse alguém é o protocolo ARP. Este é um protocolo autónomo que é inserido directamente numa trama Ethernet. O formato de uma mensagem ARP é representada pela figura 31.

A título de curiosidade, este formato é o mesmo para o protocolo RARP, *Reverse Adress Resolution Protocol*. Este protocolo é usado por exemplo por estações de trabalho *diskless*, que pretendem saber qual o seu endereço IP, dado o seu endereço físico.

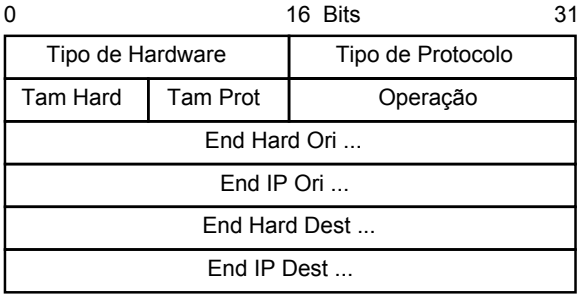


Fig 31 Formato de uma mensagem ARP

O significado dos campos é:

- Tipo de Hardware: Especifica o tipo de *interface* físico. (Ethernet=1);
- Tipo de Protocolo: especifica o tipo de protocolo de nível superior que a máquina origem especificou. (IP=0x800);

- Tam Hard: Especifica o tamanho do endereço de *hardware*;
- Tam Prot: Especifica o tamanho do endereço de nível superior;
- Operação: Especifica o tipo de operação. (Pedido ARP=1; Resposta ARP=2; Pedido RARP=3; Resposta RARP=4);
- End Hard Ori: Endereço hardware da máquina origem;
- End IP Ori: Endereço do protocolo de nível superior da máquina origem;
- End Hard Dest: Endereço hardware da máquina destino;
- End IP Dest: Endereço do protocolo de nível superior da máquina origem;

Quando uma máquina pretende comunicar com outra na mesma rede local, vai em ultima análise ter que mapear o seu endereço IP num endereço Ethernet. Para isso vai consultar a tabela mantida pelo protocolo ARP a fim de obter o endereço Ethernet correspondente ao endereço IP destino. Se esta entrada já existir na tabela o problema está resolvido e é construída a trama Ethernet. Senão, o ARP lança uma mensagem de difusão para a rede, como que pedindo: "Gostaria que a máquina cujo endereço IP é a.b.c.d, me fornecesse o seu endereço Ethernet". O pedido ARP é feito usando uma trama Ethernet, em que o campo Type contém 0x806, indicando que é uma mensagem ARP.

Como é uma mensagem de *broadcast*, todas as estações da rede a recebem. As estações cujo endereço IP não é a.b.c.d descartam o pedido. A estação a.b.c.d também recebe o pedido, inserindo, se ainda não existir, uma entrada na sua tabela de ARP, com os endereços da máquina que originou o pedido. De seguida responde com o seu endereço Ethernet.

Quando a resposta chega é adicionada à tabela da máquina que tinha originado o pedido.

As entrada de uma tabela ARP não têm uma duração ilimitada, antes pelo contrário, têm um tempo de vida findo o qual são retiradas da tabela.

5.3 O protocolo ICMP

O protocolo ICMP, *Internet Control Message Protocol*, é usado para trocar mensagens de erro e controlo ao nível do protocolo IP. As mensagens ICMP são encapsuladas em datagramas IP, isto porque pode ser necessário que atravessem várias redes, necessitando assim de um suporte de *internetworking*, o que se fossem lançadas directamente no meio físico não aconteceria. Apesar disso o ICMP não é considerado um protocolo de nível superior.

Existem 11 tipos de mensagens ICMP diferentes, sendo comum a todas apenas os primeiros 4 octetos, tal como mostra a figura 32.

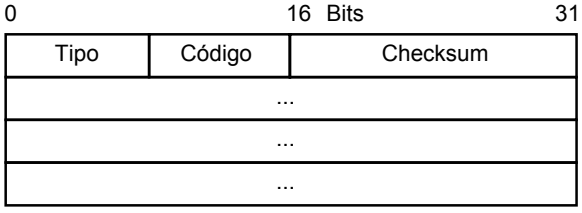


Fig 32 Campos comuns a todas as mensagens ICMP

O campo Tipo representa o tipo de mensagem ICMP. O campo código representa informação adicional para um determinado tipo de mensagem. O campo Checksum é usado para validar a correcção da mensagem ICMP. Os outros campos variam em função do tipo de mensagem.

Os vários tipos de mensagens são:

- *Echo Request/Reply*: Estas mensagens são usadas para testar se um determinado destino está activo. O comando **ping** usa esta mensagem;
- *Destination Unreachable*: Esta mensagem é enviada à máquina origem sempre que um *gateway* não consegue encaminhar um datagrama IP;
- *Source Quench*: Esta mensagem é enviada à máquina origem, quando existe congestão no *gateway*, para que esta diminua a taxa de transmissão;
- *Redirect*: Esta mensagem é enviada à máquina origem quando, esta usa um *gateway* não óptimo. A mensagem indica um *gateway* melhor para o qual a origem deve mudar o seu encaminhamento;
- *Time Exceeded for a Datagram*: Quando um *gateway* descarta um datagrama IP devido a ter chegado a zero o seu tempo de vida, uma mensagem ICMP deste tipo é enviada à máquina origem;
- *Parameter Problem on a Datagram*: Esta mensagem é enviada à máquina origem quando é detectado um erro, não coberto por outras mensagens ICMP, no datagrama IP;
- *Timestamp Request/Reply*: Usado para obter a hora da máquina destino;
- *Address Mask Request/Reply*: Mensagem usada para a máquina origem descobrir qual a máscara de rede usada;

6 O nível de transporte

Enquanto que o nível de rede da pilha OSI se preocupa em estabelecer a rota entre máquina origem e destino, o nível de transporte abstrai-se disso e vê essas as máquinas ligadas directamente.

Do ponto de vista do protocolo de transporte, o exemplo de comunicação referido aquando da discussão do protocolo IP, entre as máquinas A e D, é visto como uma ligação directa entre as máquinas, tal como se pode ver pela figura 33.

Desta forma, os níveis superiores ficam isolados da complexidade que está por baixo, vendo apenas uma ligação directa entre máquina origem e máquina destino.

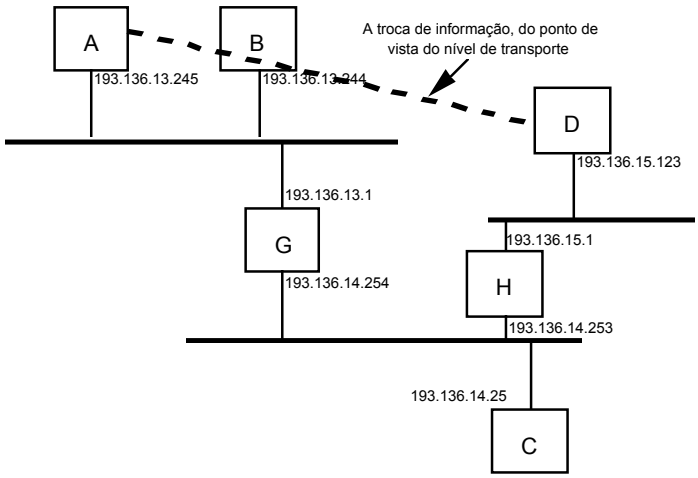


Fig 33 A comunicação ente dois sistemas do ponto de vista do nível de transporte

Tal como noutros níveis, também a comunicação no nível de transporte pode ou não ser orientada à conecção. Dois exemplos disto são os protocolos UDP e TCP, da pilha TCP/IP. Estes protocolos usam o IP como protocolo de rede.

6.1 O protocolo UDP

O UDP, *User Datagram Protocol*, é um protocolo não fiável e não orientado à conexão. À primeira vista tem portanto as mesmas características do próprio IP. Então para que serve o UDP?

O protocolo IP identifica como destino uma máquina. Não é feita mais nenhuma distinção sobre a aplicação que irá receber o datagrama. Assim, a grande diferença entre o IP e o UDP é de que este último identifica a "quem", dentro da máquina, é destinada a informação.

Como protocolo não fiável que é, o UDP passa toda a responsabilidade da validação da informação para a aplicação. Assim, questões como perca de dados, atrasos, entrega fora de ordem, etc. passam a ser da responsabilidade da aplicação e não do protocolo UDP.

6.1.1 O formato do datagrama UDP

O formato do datagrama UDP é apresentado na figura 34.

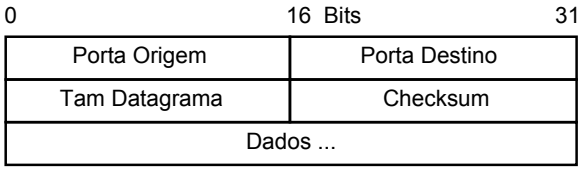


Fig 34 O formato de um datagrama UDP

Os campos têm o seguinte significado:

- Porta Origem/Destino: Serve para distinguir a quem se destina a informação dentro da máquina;
- Tam Datagrama: Representa o tamanho do datagrama;
- Checksum: Valida a informação contida no datagrama;
- Dados: Dados do nível da aplicação.

6.1.2 O cálculo do *checksum*

Este cálculo não envolve apenas a informação do datagrama. Para o seu cálculo é acrescentado no início do datagrama UDP um pseudo-cabeçalho, tal como indica a figura 35.

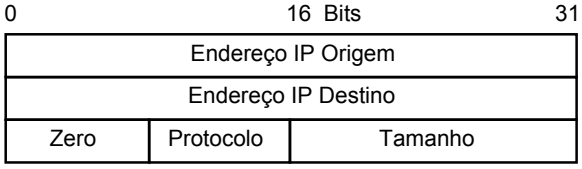


Fig 35 Pseudo cabeçalho de um datagrama UDP/TCP

Em que:

- Endereço IP Origem/Destino: Informação do sistema remetente/destino da informação;
- Zero: campo a zero;
- Protocolo: Tem um significado igual ao campo do mesmo nome no datagrama IP. Indica qual o protocolo que segue no campo de dados do IP;

- Tamanho: Representa o tamanho do datagrama UDP.

6.1.3 Well known ports

Imagine-se um banco. Este oferece vários serviços tais como, movimentar a conta à ordem, requisição de cheques, pedido de empréstimo, etc. Para ser atendido, é necessário que o cliente entre na fila correcta, senão é mandado de volta. Da mesma forma, o UDP oferece vários serviços, definindo para cada um deles uma porta de entrada.

As portas são chamadas de *well known*, pois à partida são bem conhecidas da máquina que pretende aceder a determinada informação.

Por exemplo vejamos uma aplicação de transferência de ficheiros. Se o utilizador da máquina A quiser transferir um ficheiro da máquina B, terá que existir um programa na máquina B, à espera numa determinada porta X que alguém lhe peça ficheiros para transferir. Assim, o pedido UDP vindo da máquina A terá que ser dirigido à porta X.

6.2 O protocolo TCP

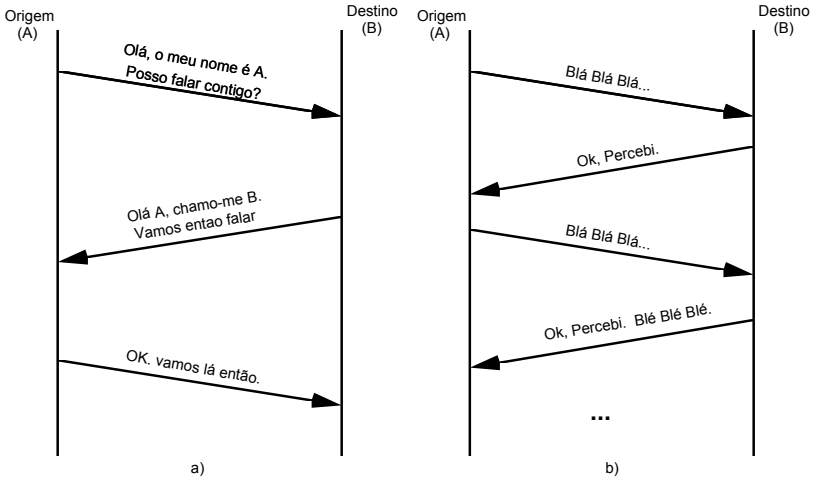
Como foi referido este é um protocolo orientado à conexão, pois para haver troca de informação entre dois sistemas tem que se abrir uma "ligação" entre si, e é um protocolo fiável, pois o receptor tem sempre que fazer o *acknowledgment* da informação recebida.

6.2.1 As conexões TCP

A "ligação" entre dois sistemas tem três fases:

- Estabelecimento da conexão.
- Transferência de informação;
- Fecho da conexão;

Estas três fases são típicas de qualquer protocolo orientado à conexão. A figura 36 representa as várias fases da conexão, com os respectivos *acknowledgments* para garantir a fiabilidade, tal como o TCP as vê.



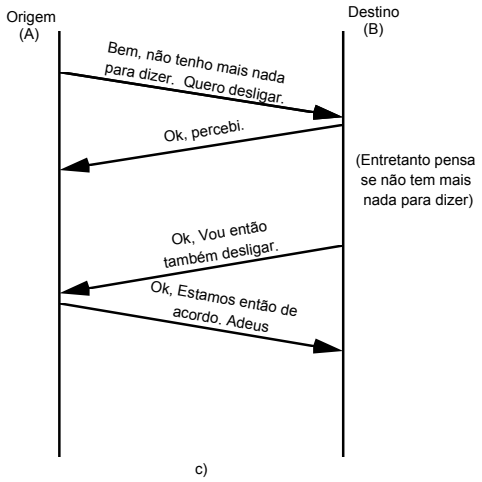


Fig 36 As três fases de uma conexão no TCP

6.2.2 O formato de um segmento TCP

O formato de um segmento TCP é apresentado na figura 37.

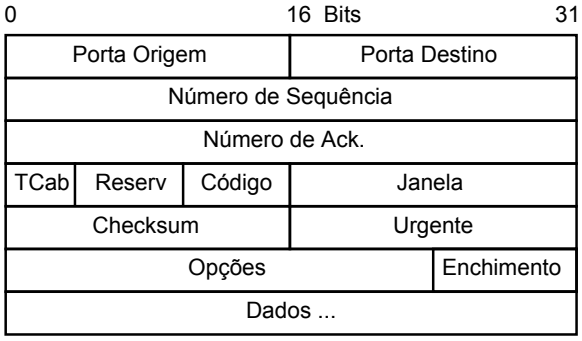


Fig 37 O formato de um segmento TCP

Os vários campos têm o seguinte significado:

- Porta Origem/Destino: Identifica os programas do nível da aplicação que estão a usar o TCP;
- Número de Sequência: Identifica a sequência numérica do primeiro octeto no campo de dados. No TCP todos os octetos de dados enviados têm uma ordem numérica usada pelo protocolo;
- Número de Ack.: Representa o número do próximo octeto esperado. Isto é, a sequência numérica do último octeto recebido mais um;
- TCab: Tamanho do cabeçalho TCP;
- Reserv: Reservado para uso futuro, deve estar a zero;
- Código: Representa operações que o segmento pode a executar. Por exemplo é necessário indicar se o segmento está a fazer *acknowledgment* de outro (*bit* ACK), se contém dados urgentes (*bit* URG), se acabou a informação a ser transmitida (*bit* FIN), etc.
- Janela: Representa o número de octetos que o remetente do segmento está disposto a aceitar. É a janela deslizante do receptor;
- Checksum: Valida a integridade do segmento. Tal como no caso do UDP é usado um pseudo-cabeçalho, como o da fig. 34, para o seu cálculo;

- Urgente: No caso de no campo Código a *flag* URG estiver activa, este campo indica o deslocamento dentro do campo dados onde essa informação urgente se encontra; Por exemplo, no caso de uma sessão Telnet, a sequência de caracteres CTRL-S e CTRL-Q devem ser imediatamente atendidas, independentemente de seguir mais informação no segmento TCP, visto representarem parar e retomar, respectivamente o *scroll* do ecrã;
- Opções: Campo, com uma utilização muito limitada, actualmente;
- Enchimento: No caso de o campo anterior existir, este campo serve para enchimento até que o campo anterior tenha 32 *bits*;
- Dados: Campo onde segue a informação do nível da aplicação;

6.2.3 Janela deslizante

O TCP usa o conceito de janela deslizante, *sliding window*, quer para optimizar a utilização do canal, quer para fazer o controlo de fluxo.

Na fig. 37 está representada uma comunicação sem janela deslizante. A origem só envia informação quando recebe o *acknowledgment* da informação anterior.

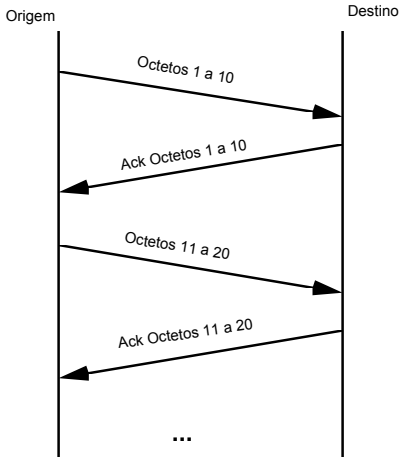


Fig 37 Comunicação sem janela deslizante

Na fig. 38 temos uma janela deslizante de dois, isto é são feitas duas comunicações sem que se espere o *acknowledgment* . Quando este começa a surgir são enviadas as comunicações seguintes. Desta forma é feito um aproveitamento muito melhor do canal de transmissão.

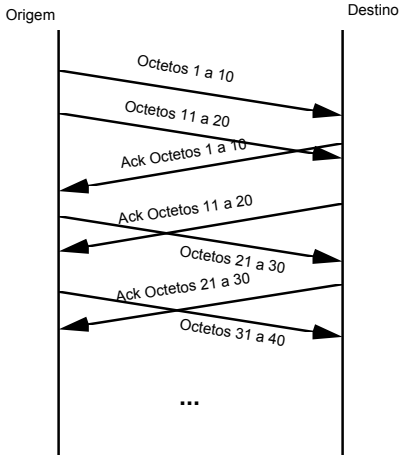


Fig 38 Comunicação com janela deslizante

Em termos de linguagem TCP diríamos que, na fig. 38, o tamanho de dados do segmento é 10 e a janela deslizante é 20 octetos. O TCP mede a janela deslizante em termos de octetos. Como cada segmento só leva 10 octetos, são necessários dois segmentos para transmitir a janela.

Até agora estivemos a lidar com uma janela deslizante de tamanho fixo. O que o TCP faz, para realizar a tarefa de controlo de fluxo é utilizar janelas deslizantes de tamanho variável.

A variação do tamanho da janela deslizante pode ser devida a dois factores:

- Por informação da máquina remota, através do campo Janela do segmento TCP. Desta forma é implementado o controlo de fluxo da máquina remota, pois a janela aumenta ou diminui em função do espaço de *buffer* disponível;
- Por perda de segmentos pela rede. Muitas vezes, perda de informação pela rede é devida ao facto de os *gateways* estarem sobrecarregados, tendo por isso que descartar pacotes.

Neste caso a dificuldade é que os sistemas finais não sabem onde estão os problemas. A abordagem mais fácil seria a de começar a fazer retransmissões da informação, o que, no caso de congestão, agravaria ainda mais os problemas.

A abordagem do TCP é diminuir a taxa de transmissão. Para isso utiliza uma janela de congestão que diminui para metade sempre que um segmento é perdido. A janela de transmissão é a menor de entre a janela recebida da máquina remota e a janela de congestão, reduzindo assim rápida e significativamente o tráfego na rede. As retransmissões que tiver que fazer dos segmentos da janela, usam um algoritmo de retirada exponencial. Quando a congestão termina é adoptado um algoritmo de *slow-start*, em que a janela de congestão aumenta lentamente.

6.2.4 Timeout e acknowledgment

O valor de *timeout* , dado para a recepção de um *acknowledgment* , não é constante, mas antes é adoptado um modelo de transmissão adptativa. Isto é, é monitorizado o tempo médio entre o envio de um segmento e a chegada do *acknowledgment*. Desta informação, é calculado um novo valor de *timeout*. Sempre que existe *timeout* é novamente enviado o primeiro segmento da janela de transmissão.

Em relação ao *acknowledgment*, este é feito de uma forma comulativa, tal como se vê na fig. 39. Só é feito *acknowledgment* da informação correctamente ordenada. Na fig. 39 b) e c) nova informação fora de ordem chegou, mas só quando chega o segmento que faltava é que implicitamente todos os segmentos são acusados, tal como se apresenta em d).

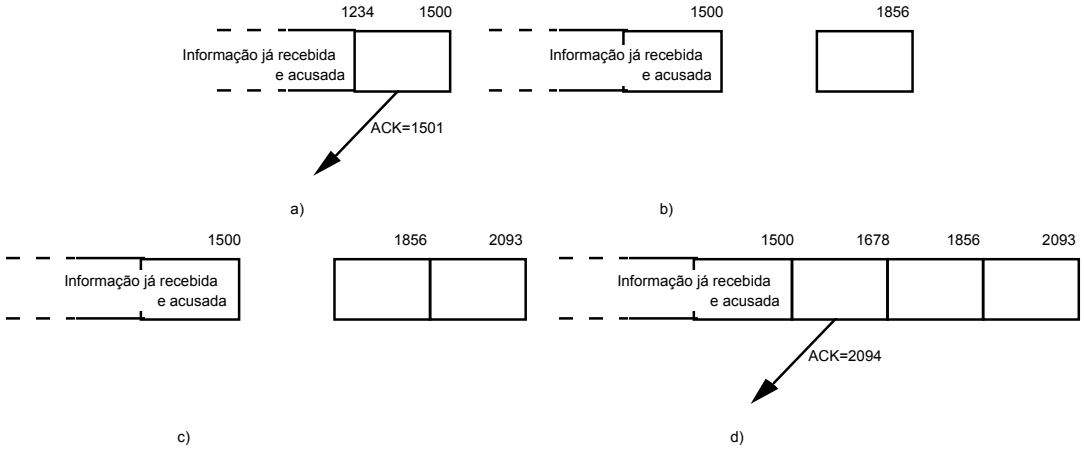


Fig 39 *Acknowledgment* comulativo

6.2.5 *Well known ports*

Tal como no UDP existe a noção de *well known ports*. No entanto e devido à noção de conexão introduzida pelo TCP estas portas não são simples filas de entrada da informação pois podem suportar mais do que uma conexão ao mesmo tempo. Além disso, cada conexão é identificada pelo par endereço, IP porta de acesso.

Vejamos um exemplo. A máquina A pretende ir buscar um ficheiro, via ftp, à máquina B. Para isso abre uma conexão com a *well known port* 21 da máquina B. A partir dessem momento está aberta a conexão (A,21), na máquina B. Esta, "vê" que a máquina A está a ligar-lhe a partir da porta 1029. Estabelece-se assim a conexão (B,1029). A partir daqui pode-se dar a transferência do ficheiro.

Se por exemplo a máquina C pretende também aceder à máquina B vai estabelecer com esta a conexão (C,21).

Pode-se reparar que mesmo estando várias máquinas a aceder à mesma *well known port* na máquina destino estabelecem conexões diferentes e nunca a máquina destino se poderá confundir com vários clientes ao mesmo tempo.

6.3 O protocolo NetBEUI

Para finalizar vamos introduzir o NetBEUI. É um protocolo desenvolvido pela IBM em 1985 e é uma implementação da especificação NetBIOS. É usado, entre outros, pelos produtos Lan Manager, Windows for Workgroups, Windows 95, WorkGroup Connection e Windows NT da Microsoft. O modelo completo implementado para suporte às redes Microsoft é apresentado na figura 40.

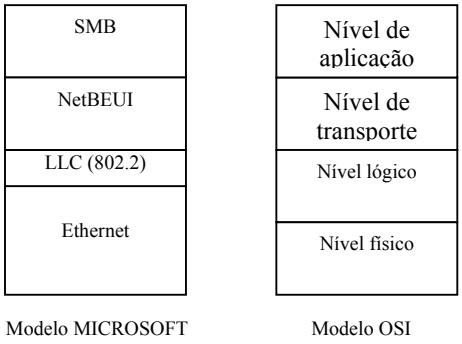


Fig 40 Posição do NetBEUI no modelo OSI

As aplicações, através das funcionalidades definida pelo NetBIOS usam o NetBEUI e os serviços por este suportados.

É um protocolo que suporta o modo de comunicação fiável e orientado à conexão, bem como o modo datagrama, não fiável e não orientado à conexão. Este modo é usado quando é necessário fazer *broadcast* e/ou *multicast*.

Estes modos de funcionamento são garantidos não pelo NetBEUI em si mas sim pelo pela sub-camada LLC do nível 2, neste caso o 802.2.

Pelo modelo apresentado, vemos que o NetBEUI é um protocolo que não suporta *internetworking*. Assim se numa *internet* for necessário estabelecer comunicação entre máquinas será necessário encapsular o NetBIOS numa outra plataforma, que permita fazer o encaminhamento.

7 O nível de Sessão e nível de Apresentação

Estes dois níveis OSI estão bastante ligados com as aplicações, por isso muitas vezes a sua funcionalidade está diluída nas aplicações.

7.1 O nível de Sessão

Se até agora os protocolos viam os sistemas como destinatários da informação, a função principal do protocolo de sessão é fazer com que duas entidades do nível de aplicação possam comunicar entre si, estabelecendo um canal de comunicação para a troca de informação.

Como se vê é conceptualmente a partir daqui que a comunicação se torna individualizada entre duas entidades do nível de aplicação. Assim, o nível de sessão é responsável pela multiplexagem da informação vinda das entidades do nível de aplicação passando a informação para os níveis inferiores, fazendo a operação inversa aquando da chegada de informação.

7.2 O nível de Apresentação

Este nível é responsável pela representação da informação durante a transferência entre duas aplicações remotas. É a este nível que se negoceia o tipo de sintaxe de transferência. Esta sintaxe de transferência tem por fim esconder as particularidades intrínsecas a cada aplicação ou sistema na forma como representam a informação.

Por exemplo suponhamos que um sistema A suporta inteiros de 4 bytes e outra máquina B suporta inteiros de 2 bytes. Imaginemos agora que uma aplicação na máquina A quer enviar o valor numérico 2 para a máquina B. Esta máquina está à espera de receber 2 bytes e recebe 4, podendo interpretar mal a informação recebida. Por isso seria importante que existisse "alguém" na máquina A que convertesse essa informação para uma notação independente de qualquer sistema, para que depois, do lado da máquina B, outro "alguém" que percebesse essa notação a pudesse converter sem ambiguidades para a notação local da máquina.

Um exemplo ainda mais simples é a conversão do fim de linha num sistema UNIX para o fim de linha num sistema MS-DOS.

Este "alguém" seria um protocolo de nível de apresentação.

Outras utilizações do protocolo de apresentação são por exemplo, a compressão de dados e a criptografia.

Um exemplo de protocolo de apresentação é o protocolo XDR, eXternal Data Representation, criado pela SunSoft. Este protocolo permite a descriçãode estruturas de dados arbitrárias em termos independentes da máquina.

8 O nível de Aplicação

Este nível não são as aplicações!!! Este nível suporta as aplicações. O seu objectivo é fornecer serviços de comunicações às aplicações. Estabelece e controla o ambiente no qual as aplicações realizam as suas tarefas.

Por exemplo o SMTP, *Simple Mail Transfer Protocol*, é um protocolo de nível de aplicação que implementa um serviço de correio electrónico. Não é a aplicação em si. Aplicações de correio electrónico existem várias mais ou menos amigáveis, tendo todas como denominador comum a implementação do protocolo SMTP.

8.1 O conceito cliente/servidor

Este é um conceito muito importante e no qual se baseiam todas as aplicações de rede.

Este conceito vai muito mais além do que " Aquele computador é um servidor". É um conceito que se aplica às aplicações.

Num sistema UNIX, por exemplo, podem simultaneamente estar a executar aplicações servidoras e clientes.

Basicamente, cliente é a aplicação que solicita um serviço e servidor é a aplicação que o fornece.

Um exemplo é dado pela utilização do programa **telnet**. Quando fazemos **telnet** para um sistema, é usado o TCP que liga a uma *well known port*, na máquina remota. Associada a essa *well known port*, está um programa, **telnetd** nos sistemas UNIX, que aguarda em *backgroud* conexões de terminal remoto. Neste caso o **telnetd** é o servidor e o nosso programa **telnet** é o cliente.

Toda a comunicação no TCP/IP baseia-se neste paradigma cliente/servidor, em que não são os sistemas que definem o conceito mas as aplicações.

Parte II - Os sistemas operativos de rede e as aplicações

Todos os conceitos apresentados anteriormente tem como fim último poderem ser usados pelos sistemas operativos e pelas aplicações.

Existem vários tipos de arquitecturas de rede com os seus objectivos específicos. Em última análise pretende-se de alguma forma comunicar e partilhar recursos, seja comunicar através da troca ficheiros e correio electrónico ou partilhar impressoras, ficheiros em disco ou mesmo poder computacional.

Nos primeiros tempos das redes, nos reino dos *mainframes* e grandes sistemas, estas eram usadas principalmente nas grandes organizações e em núcleos mais ou menos restritos tais como os meios académicos, para fazer terminal remoto, transferência de ficheiros e correio electrónico. Como exemplo de uma arquitectura usada neste ambiente temos a plataforma aberta TCP/IP e os proprietários DECnet. da DEC e SNA da IBM.

Com o advento do PC e da sua banalização começam também nas pequenas empresas e escritórios a surgir a necessidade de interligar os equipamentos para troca de informação e partilha de recursos. Temos como exemplos destas arquitecturas o NetWare da Novell, o Windows for Workgroups e Windows 95 da Microsoft, etc.

Actualmente coexistem estes dois tipos de plataformas tendo cada uma um fim específico.

Vamos agora introduzir alguns serviços oferecidos por estas plataformas.

1 O TCP/IP

Este é talvez o protocolo mais usado. Basta para isso dizer que quando se fala em INTERNET estamos a falar de uma mega-rede que usa o TCP/IP.

Tal como já foi referido inicialmente eram oferecidos basicamente serviços de terminal remoto, transferência de ficheiros e correio electrónico. Actualmente, uma miríade de protocolos e serviços usam esta plataforma. vamos passar a ver alguns deles.

1.1 O TELNET

Protocolo que implementa a noção de terminal remoto no TCP/IP. O utilitário que usa este protocolo tem o geralmente o mesmo nome.

1.2 O FTP

O *File Transfer Protocol* implementa a transferência de ficheiros. O utilitário que usa este protocolo tem o geralmente o mesmo nome.

1.3 O SMTP

O *Simple Mail Transfer Protocol*, implementa o serviço de correio electrónico. Em UNIX o utilitário que implementa este protocolo geralmente chama-se **mail**.

1.4 O DNS

O *Domain Name System*, implementa uma noção importante no TCP/IP, que é a noção de nome. Para o TCP/IP um sistema é identificado por um endereço IP. No entanto para os humanos é mais fácil a memorização de um nome. No entanto como o TCP/IP apenas conhece endereços IP é necessário que "alguém", o DNS, faça a conversão de nomes para endereços. A isto chama-se resolução de nomes.

Para realizar esse objectivo o DNS criou sistema hierárquico de nomes. Por exemplo o nome **zeca.eng.uminho.pt** representa a máquina **zeca** que faz parte da sub-organização **eng**, que por sua vez faz parte da organização **uminho** que por sua vez faz parte da organização **pt**. Em termos de DNS estas organizações chamam-se domínios, e cada domínio tem um servidor de nomes. Esta organização é uma organização lógica, não tendo necessariamente a ver coma localização física. Por exemplo o nome emb1.emb-br.mne.pt poderia referir-se a uma máquina localizada no Brasil, pertencendo no entanto ao domínio pt.

Para se perceber como é feira a resolução de nomes, vejamos um exemplo. Quando a partir da nossa máquina queremos aceder à máquina **ftp.ul.ao**, o *resolver* da nossa máquina consulta o *name server* para o qual está dirigido, por configuração local. Se o *name server* tiver a máquina remota na sua *cache* responde, indicando o respectivo endereço IP. Senão, vai consultar um *root server*, sistema que está no topo da hierarquia. Este vai questionar o servidor de **ao**, que por sua vez consulta o servidor de **ul**. Este servidor, finalmente, vai responder à nossa máquina indicando qual o endereço IP de **ftp.ul.ao**.

O servidor de nomes nas máquinas UNIX geralmente tem o nome de **named**. Existe também um utilitário, o **nslookup**, que permite fazer questões aos *name servers*.

1.5 O NFS

O *Network File System* é um protocolo desenvolvido pela Sun Microsystems Inc. que permite a partilha de ficheiros de uma forma transparente. Um máquina vê uma determinada directoria remota partilhada, como se fosse uma sub-directoria local.

O NFS assenta a sua estrutura em dois conceitos bastante importantes RPC, *Remote Procedure Call*, e XDR, *eXternal Data Representation*. Estes dois conceitos são muito importantes para a noção de processamento distribuído.

1.6 O X-Windows

É um ambiente gráfico que permite fazer o *display* remoto de aplicações.

1.7 O SNMP

O *Simple Network Management Protocol*, é um protocolo de gestão de redes.

1.8 O HTTP

O *HyperText Transfer Protocol* é actualmente a "coqueluche" de quem quer navegar na Internet. Conhecidos programas como o **Mosaic**, o **Netscape** e o **Internet Explorer** usam este protocolo.

2 As arquitecturas de redes locais

Como já foi referido, com o advento e banalização dos Pcs novas necessidades se põem às arquitecturas de redes. Surgem assim implementações mais amigáveis e melhor adaptadas a estes ambientes.

Em relação a estas arquitecturas podemos ainda dividi-las em duas categorias, *File Servers* e *Peer-to-Peer*.

2.1 File Servers

Um arquitectura baseada neste conceito é uma arquitectura em que existe um computador, geralmente com características muito superiores aos outros, e que faz o papel de servidor. Seja servidor de disco, de impressão, etc.

As outras máquinas que estão na rede, os clientes, se quiserem aceder a esses recursos têm que se ligar, através de *drives* lógicos por exemplo, ao servidor.

Como exemplos destas arquitecturas temos:

- Netware da Novell;
- Vines da Banyan;
- AppleShare da Apple;
- Lan Manager da Microsoft;
- Windows NT da Microsoft;

As funções principais destes servidores é:

- Fornecer serviços de ficheiros e de impressora;
- Controlar o acesso dos clientes aos seus serviços;
- Gerir os acessos múltiplos dos clientes;

2.1.1 Windows NT

O sistema Windows para ambientes empresariais é o Windows NT. Poderemos de uma forma simples dizer que este sistema é idêntico ao sistem Windows 95 mas com mecanismos de segurança. Por um lado, um utilizador só pode aceder ao sistema se estiver registado no domínio. Por outro lado, todos os ficheiros e directorias podem ser protegidos de forma restringir ou negar o seu acesso.

Em termos de rede, o conceiro de *workgroup* é substituído pelo conceito de domínio. Enquanto que no Windows 95 qualquer máquima pode pertencer a um grupo de trabalho, para que uma máquina NT possa pertencer a um domínio, terá que ser "autorizada" pelo administrador do domínio. Existe assim uma hieraquia dentro de um domínio NT. Por um lado existe uma máquina que é controladora de domínio, designada por Primary Domain Controller. Poderão existir outras máquinas de *backup*, controladoras de domínio designadas por Backup Domain Controller. O sistema operativo a instalar nestas máquinas é o Windows NT Server. Poderão existir outras máquinas Windows NT Server que não sejam controladoras de domínio mas que sejam servidoras, por exemplo de WWW, DNS, etc.

As máquinas dos utilizadoras terão o sistemas Windows NT Workstation. Estas são idênticas aos servidores excepto que não possuem de base um conjunto de serviços.

Como já foi referido todos os utilizadores têm que ter uma conta no domínio para poderem aceder às máquinas. Existe uma conta especial, o administratador que tem privilégios e que se

esse administrador for da máquina que é o Primary Domain Controller então chama-se administrador do domínio. Todas as máquias poderão ter administradores locais.

Será tarefa do administrador de domínio a criação/remoção das contas dos utilizadores bem como a inserção/remoção de máquinas no domínio. O administrador possui privilégios totais sobre as máquinas quer para alterar configurações quer para aceder a qualquer área de ficheiros.

A configuração das placas de rede bem como dos protocolos é muito parecida com a realizada no Windows 95.

2.2 Arquitecturas *Peer-to-Peer*.

Podemos traduzir *peer-to-peer*, por par-a-par, pois é isso mesmo que se passa. Numa arquitectura deste género todas as máquinas estão ao mesmo nível, podendo ser servidores e clientes ao mesmo tempo.

Como exemplos destas arquitecturas temos:

- Macintosh System 7 da Apple;
- LANtastic da Artisoft;
- Personal NetWare da Novell;
- Windows for Workgroups e Windows 95 da Microsoft.

Algumas vantagens destas arquitecturas são:

- Baixo custo. São substancialmente menos onerosas que as arquitecturas baseadas em *file server*;
- Flexibilidade. Facilmente são disponibilizados recursos em qualquer sistema;
- Simplicidade. São mais simples de instalar e gerir que a outra arquitectura;

No entanto, têm também desvantagens:

- Desempenho. São mais lentos que os servidores dedicados;
- Está sob o controlo do utilizador, como todas as consequências quer em termos de manutenção do serviço, quer em termos de segurança.

Apesar de tudo, devido ao seu baixo custo e desempenho razoável, são uma boa solução para as pequenas organizações.

2.2.1 Windows for Workgroups

Este produto é basicamente o sistema Windows 3.1 com capacidades de rede.

Na fase de instalação, o Windows for Workgroups, WfWg, é necessário fornecer ao computador um nome, pelo qual vai ser conhecido na rede, e um grupo de trabalho, *workgroup*, a que pertence.

Associado a cada computador vai estar um par *login*, *password*, que permite automatizar o acesso a recursos remotos.

Em termos de configuração esta é gerida por dois utilitários **Network Setup** e **Control Panel**. Através do **Network Setup**, são inseridos e configurados, quer os *drivers* das placas, quer os protocolos. No **Control Panel** através do ícone Network, pode-se por exemplo, alterar o nome e o grupo de trabalho a que o computador pertence.

Em termos de funcionalidade do sistema, grande parte está no **File Manager** e **Print Manager**. Através do **File Manager** é possível abrir aceder a directorias remotas partilhadas, como se fossem *drives* locais, através da utilização de uma opção da barra de ferramentas. Uma outra opção dessa barra permite a partilha para a rede de directorias locais. O **Print Manager** permite as mesmas operações mas em relação a impressoras.

Outras aplicações são:

- Chat: Permite a comunicação interactiva entre utilizadores em máquinas diferentes;
- WinWatcher: Vigia a utilização dos recursos locais, por parte de utilizadores remotos;
- WinMeter: Monitoriza a utilização dos recursos locais por parte da rede;
- Clipbook Viewer: Uma espécie de *clipboard* de rede.

2.2.2 Windows 95/98

O sucessor do Windows Windows for Workgroups foi o Window 95. Esta nova versão do Windows, apesar de alterar drasticamente o ambiente de trabalho usa os mesmos conceitos de rede do sistema anterior.

Assim tal como no WfWg existem, em termos de configuração do ambiente de rede do Windows 95, dois conceitos fundamentais:

- Nome da máquina. Representa o nome pelo qual a máquina vai ser conhecida na rede;
- Grupo de trabalho. Indica o grupo a que a máquina pertence. Este conceito define uma organização lógica para as máquinas na rede. Assim, em vez de as máquinas estarem todas ao mesmo nível, em termos de visualização para o utilizador, estão divididas em grupos, em que cada grupo tem um nome. Esta divisão em grupos é puramente formal e não tem qualquer significado em termos de acesso a outras máquinas de outros grupos e seus respectivos recursos partilhados.

Associado a cada computador vai estar um par *login*, *password*, que permite automatizar e autorizar o acesso a recursos remotos.

Em termos de configuração esta é gerida pelo utilitário `Network` que se encontra em `Start`→`Settings`→`Control Pannel`. É através deste utilitário que é feita toda a gestão de rede do computados, isto é, a instalação, alteração de configuração e remoção das placas de rede, protocolos e serviços.

Em termos de funcionalidade do sistema, grande parte está no `Network Neighborhood`, que se encontra no *desktop*, `Windows Explorer`, que se encontra em `Start`→`Programs` e na gestão das impressoras feita através de `Start`→`Settings`→`Printers` ou `Start`→`Settings`→`Control Pannel`→`Printers`.

Através do `Windows Explorer` é possível fazer com que uma directoria remota partilhada possa ser vista como num *drive* da máquina local, através da utilização de uma opção da barra de ferramentas. Uma outra opção dessa barra permite a partilha para a rede de directorias locais.

O `Network Neighborhood` permite o acesso a directorias remotas, sem ser necessária a criação de *drives* de rede.

A gestão das impressoras permite a utilização de uma impressora remota bem como a partilha de impressoras locais.

Outras aplicações são listada para o WfWg estão também no Windows 95.

Um pequeno pacote que pode ser utilizado em máquinas que não permitam o WfWg ou o Win 95, mas que tenham necessidade de aceder aos recursos da rede, é o Workgroup Connection, WgC. Este pequeno pacote permite apenas a ligação a recursos partilhados na rede, não havendo hipótese de partilhar os recursos locais.