

Endereçamento IP

Para que uma rede funcione, é necessário que os terminais dessa rede tenham uma forma de se identificar de forma única. Da mesma forma, a interligação de várias redes só pode existir se as redes estiverem, também, identificadas no seu conjunto. Essa forma de identificação utilizada nas redes de computadores actuais é o chamado Endereço IP.

Actualmente, existem duas versões de endereço IP: a versão 4 (IPv4) e a versão 6 (IPv6). A diferença entre elas é a quantidade de bits que compõe um endereço e, por conseguinte, a quantidade de redes e computadores possíveis de endereçar. Vamo-nos concentrar na versão 4, que é a mais utilizada, uma vez que a versão 6 é apenas a resposta ao número crescente de computadores ligados em rede. Por isso, a partir deste ponto, “endereço IP” refere-se apenas a um endereço IP versão 4 (IPv4)

O endereço IP (v4) é um número de 32 bits com 4 conjuntos de 8 bits ($4 \times 8 = 32$). A estes conjuntos de 4 bits dá-se o nome de **octeto**.

Um exemplo de um endereço IP é: **192.168.1.10** .

Podemos dizer que um endereço IP tem duas partes:

- a identificação da **REDE**
- a identificação do **HOST** dentro dessa rede (host é um terminal, um nó da rede – um computador, impressora, router, switch...)

Nota: é de referir que o endereço IP não identifica propriamente uma máquina mas sim uma ligação à rede. Ou seja, se um router, por exemplo, tiver 2 computadores ligados, ele terá um IP por cada porta onde tem ligado um computador. Por outras palavras, se o nosso router for um computador, esse computador terá de conter duas placas de rede, cada uma definida com um IP diferente.

Voltando aos endereços...

Um número de 8 bits permite ter até 256 (0 a 255) combinações diferentes. Isto é, se o endereço tem 4 conjuntos de 8 bits, teoricamente podemos ter 4×256 números para representar redes/hosts.

Nota: Na verdade, a quantidade de IPs disponíveis para cada octeto é menor, uma vez que os endereços 0 e o 255 não são permitidos. Ou seja, não podemos ter endereços do tipo: 0.10.120.23 ; 129.19.29.255 ; 0.0.10.14

Como já foi dito, o endereço IP é dividido em duas partes. A primeira identifica a rede à qual um equipamento está ligado e a segunda identifica esse equipamento dentro dessa rede. Assim, os primeiros octetos servem sempre para identificar a rede e os últimos octetos para identificar as máquinas(hosts). Como temos apenas 4 octetos, se fosse reservado apenas o primeiro octeto, teríamos um grande número de hosts ($256 \times 256 \times 256$) mas um pequeno número de redes (256). Mesmo que reservássemos dois octetos para as redes, os endereços possíveis seriam insuficientes.

Assim, foram definidas **classes de endereços**, de modo a permitir uma maior gama de endereços. Foram definidas 5 classes: A,B,C,D,E. Vamos concentrar-nos nas primeiras três classes:

Classe A → apenas o primeiro octeto identifica a rede e os últimos três octetos identificam os hosts; isto quer dizer que poderíamos ter, no máximo, 254 (o 0 e o 255 não contam) redes e $256 \times 256 \times 254$ (**ver figura 2**)

Classe B → os dois primeiros octetos identificam a rede e os outros dois identificam os hosts; neste caso, podemos ter mais redes, mas menos hosts em cada rede

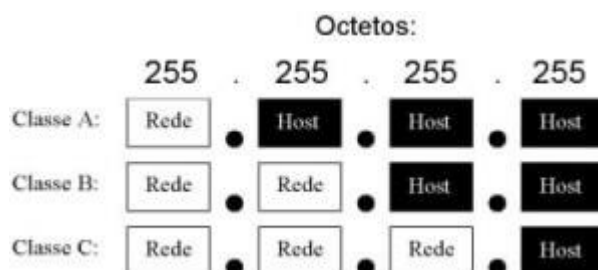
Classe C → os três primeiros octetos identificam as redes possíveis e apenas o último octeto identifica os hosts; aqui, podemos ter muito menos hosts em cada rede (254), mas muitas redes...

É fácil de ver que os endereços de classe C são mais adequados a redes com poucos computadores (como as redes locais, por exemplo) e que os endereços de classe A para redes com muitos computadores...

O que diferencia uma classe de endereços de outra é o valor do primeiro octeto. Assim, em relação ao primeiro octeto:

A – entre 1 e 126	B – entre 128 e 191	C- entre 192 e 224
-------------------	---------------------	--------------------

*Nota: se reparares, há um salto entre o 126 e o 128; isto acontece porque os endereços entre 127.0.0.0 e 127.255.255.255 estão reservados para **loopback** (ver quadro na página seguinte)*



Ao instalar uma rede TCP/IP é necessário analisar qual classe de endereços mais adequada, baseado no número de nós da rede. Por exemplo, com um endereço classe C, é possível endereçar apenas 254 nós de rede; com um endereço B já é possível endereçar até 65,534 nós e com endereços de classe A é possível endereçar até 16,777,214.

Nota: a classe C é a classe mais comum..

Vejamos alguns exemplos de endereços IP válidos:

Classe A	105.216.56.185	45.210.173.98	124.186.45.190	89.42.140.202	34.76.104.205
Classe B	134.65.108.207	189.218.34.100	156.23.219.45	167.45.208.99	131.22.209.198
Classe C	222.45.198.205	196.45.32.145	218.23.108.45	212.23.187.98	220.209.198.56

E alguns exemplos de endereços não permitidos:

Endereço inválido	Por que?
0.xxx.xxx.xxx	Nenhum endereço IP pode começar com zero, pois o identificador de rede 0 é utilizado para indicar que se está na mesma rede, a chamada rota padrão.
127.xxx.xxx.xxx	Nenhum endereço IP pode começar com o número 127, pois este número é reservado para testes internos, ou seja, são destinados à própria máquina que enviou o pacote. Se por exemplo você tiver um servidor de SMTP e configurar seu programa de e-mail para usar o servidor 127.0.0.1 ele acabará usando o próprio servidor instalado máquina :-)
255.xxx.xxx.xxx xxx.255.255.255 xxx.xxx.255.255	Nenhum identificador de rede pode ser 255 e nenhum identificador de host pode ser composto apenas de endereços 255, seja qual for a classe do endereço. Outras combinações são permitidas, como em 65.34.255.197 (num endereço de classe A) ou em 165.32.255.78 (num endereço de classe B).
xxx.0.0.0 xxx.xxx.0.0	Nenhum identificador de host pode ser composto apenas de zeros, seja qual for a classe do endereço. Como no exemplo anterior, são permitidas outras combinações como 69.89.0.129 (classe A) ou 149.34.0.95 (classe B)
xxx.xxx.xxx.255 xxx.xxx.xxx.0	Nenhum endereço de classe C pode terminar com 0 ou com 255, pois como já vimos, um host não pode ser representado apenas por valores 0 ou 255. Os endereços xxx.255.255.255 xxx.xxx.255.255 e xxx.xxx.xxx.255 são sinais de broadcast que são destinados simultaneamente à todos os computadores da rede. Estes endereços são usados por exemplo numa rede onde existe um servidor DHCP, para que as estações possam receber seus endereços IP cada vez que se conectam à rede.

Endereços de rede privada

Dos mais de 4 bilhões de endereços disponíveis, três faixas de endereços são reservadas para redes privadas (uma para cada classe). Os endereços que estão dentro destas faixas não podem ser encaminhados (“roteados”) para fora da rede privada – ou seja, não podem comunicar diretamente com redes públicas (ex: a Internet). Dentro das classes A, B e C foram reservadas redes (norma RFC 1918) que são conhecidas como endereços de rede privados.

Estes blocos de endereços são os que devem ser utilizados, por exemplo, nas redes domésticas (ou em empresas, escolas, etc...).

A seguir são apresentados as três faixas reservadas para redes privadas:

Faixa de endereços de rede privada para cada classe:	Início	Fim	Nº de redes	Nº total de hosts
A	10.0.0.0	10.255.255.255	1	16,777,216
B	172.16.0.0	172.31.255.255	16	1,048,576
C	192.168.0.0	192.168.255.255	256	65,536

Qualquer um desses blocos de endereços pode ser utilizado, por exemplo, em redes domésticas/empresariais ou até ambientes industriais (para interligar máquinas). Normalmente o administrador de rede divide um bloco em sub-redes.

Muitos routers domésticos definem automaticamente um bloco/faixa de endereços entre 192.168.0.0 e 192.168.0.255 (endereços privados de classe C).

Na sala de aula, por exemplo, os endereços dos computadores (hosts) são do tipo 10.0.0.0 – 10.0.0.255 ; optou-se por utilizar endereços privados de classe A.

Máscaras de sub-rede (*subnet mask*)

Uma máscara de sub-rede é um número de 32 bits, dividido em 4 octetos, usado para dividir um endereço IP em sub-redes e especificar o número de hosts disponíveis em cada uma dessas sub-redes.

Uma sub-rede é uma divisão de uma rede de computadores. A divisão de uma rede grande em menores resulta num tráfego de rede reduzido, administração simplificada e melhor performance de rede.

Nota: Numa máscara, normalmente, 2 bits são atribuídos automaticamente. Por exemplo, em 255.255.255.0, o “0” é o endereço da rede e em 255.255.255.255 é o endereço de broadcast. Por isto, um endereço IP não pode conter, na parte que identifica os hosts, o valor 0 ou 255.

Como vimos antes, para facilitar o endereçamento, os endereços IP são divididos em duas partes:

- O **endereço (número) da rede** que identifica a rede/subrede: o endereço de todos os nós de uma subrede começam com a mesma sequência
- O **endereço (número) do host** que identifica uma ligação a uma máquina em particular ou uma interface desta rede.

Isto funciona de maneira semelhante a um endereço postal onde o endereço de rede representa a cidade e o endereço do host representa a rua. A máscara de subrede é usada para determinar que parte do IP é o endereço da rede e qual parte é o endereço do host.

E como é isso feito?

Os 32 bits das máscaras de sub-rede são divididos em duas partes:

- um bloco de 1s que indica a parte da rede → 11111111 (binário) é representado por 255 (decimal)
- um outro bloco de 0s que indica a parte dos hosts → 00000000 binário é 0 (decimal)

Quando alteramos a parte dos 0s, dependendo da quantidade de 0s que trocamos por 1s, estamos a dizer a quantidade de sub-redes que queremos criar. Ao mesmo tempo, definimos o número de hosts dessas redes (são os bits que sobram).

Nota: procura informação sobre conversão entre decimal e binário (já foi falado em outra altura...)

Para perceber melhor tudo isto, vejamos o seguinte exemplo:

Tomemos como exemplo um endereço de classe C (sendo x igual a 0 ou 1) e dois bits movidos para a direita para criar uma sub-rede:

endereço classe C: xxxxxxxx.xxxxxxxx.xxxxxxxx.00000000

máscara: 11111111.11111111.11111111.11000000

Ao acrescentarmos dois bits a 1 (um), podemos criar $2^2 = 4$ sub-redes. Sobram 6 zeros, logo, com esta máscara, podemos endereçar $2^6 = 64$ endereços por sub-rede. Como temos que subtrair 2 endereços (o endereço de rede, “0”, e o de broadcast, “255”), temos um total de 62 endereços de hosts ($64 - 2 = 62$).

A máscara a aplicar é 255.255.255.192, porque $256 - 64 = 192$

Então, para configurarmos uma rede/sub-rede de classe C com 62 hosts possíveis, teríamos de definir (para os hosts), algo deste género:

Computador A

IP: 194.168.1.10

Máscara: 255.255.255.192

Computador B

IP: 194.168.1.20

Máscara: 255.255.255.192

Nota: a máscara de sub-rede mais comum em redes locais é a 255.255.255.0.

Outro exemplo:

Ligação de rede sem-fios:

IP: 192.168.1.10

Máscara: 255.255.255.0

Gateway: 192.168.1.1 *(endereço da máquina que liga à Internet)

Ligação de rede de área local (com fios)

IP: 10.0.0.1

Máscara: 255.0.0.0

Gateway: 0.0.0.0

Neste exemplo, temos duas ligações de rede – uma com fios e outra, sem fios. Na ligação sem fios temos definido o GATEWAY, que é o endereço do router que liga à Internet (*ver mais abaixo). No entanto, se quisermos ligar um outro equipamento através de um cabo de rede ao mesmo computador e, mesmo assim, manter a ligação à Internet, poderíamos definir um IP e uma Máscara diferentes..ao fazermos isto, estaríamos a “criar duas sub-redes” completamente diferentes, no mesmo computador.

Alguns conceitos relacionados com Endereços IP que são importantes saber para conseguir configurar correctamente um host numa rede (e a própria rede)

Gateway

É uma máquina geralmente destinada a interligar redes ou mesmo traduzir protocolos. Exemplos de gateway podem ser os routers e as firewalls, já que ambos servem de intermediários entre o utilizador e a rede. Assume-se que o gateway tenha acesso ao exterior (ligação à Internet, por exemplo). Poderá ter também medidas de segurança contra invasões externas.

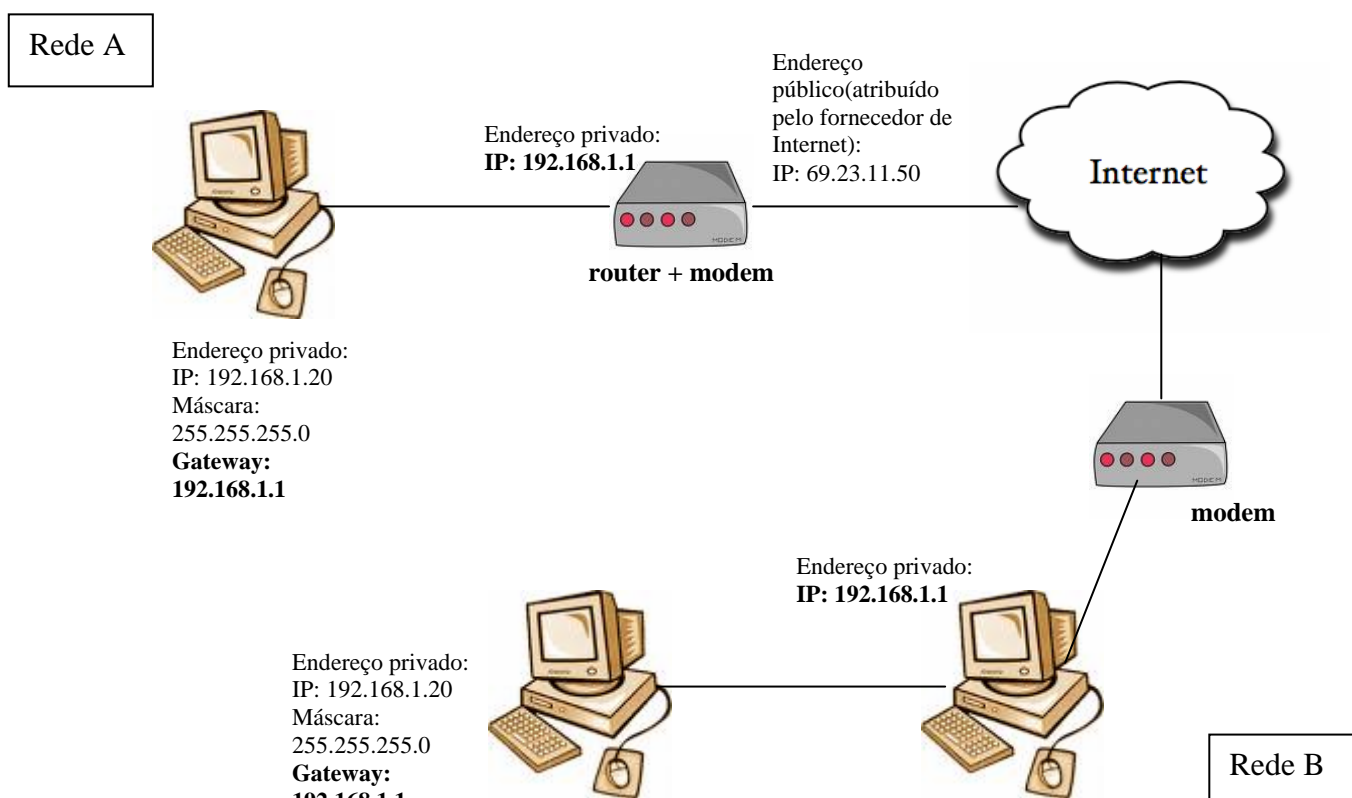
Cabe igualmente ao gateway traduzir e adaptar os pacotes originários da rede local para que estes possam atingir o destinatário, mas também traduzir as respostas e devolvê-las à origem da comunicação. Um protocolo de utilização frequente é o NAT — que é uma das implementações de gateway mais simples.

NOTA: Em redes de computadores, NAT (Network Address Translation), é uma técnica que consiste em reescrever os endereços IP de origem de um pacote que passam por um router ou firewall de maneira que um computador de uma rede interna (privada) tenha acesso ao exterior (rede pública).

Por exemplo:

- se tivermos um *router* ligado a um *modem* (que, por sua vez, liga à Internet), então esse *router* é o Gateway da nossa rede.
- se tivermos um computador ligado à Internet (ligado directamente a um *modem* ou através de um router ou outro equipamento) e estivermos a partilhar essa ligação a um outro computador que está ligado (com cabo cross-over) ao primeiro computador, então o nosso Gateway será o computador que está ligado à Internet.

Ou seja, se quisermos que um computador numa rede tenha acesso à Internet, por exemplo, teremos de definir o endereço IP do Gateway desse computador.



DHCP

Dynamic Host Configuration Protocol, é um protocolo (que faz parte do conjunto de protocolos TCP/IP) que oferece configuração dinâmica de terminais, ou seja, fornece automaticamente endereços IP de host e outros parâmetros de configuração para clientes de rede. Normalmente, um router como os utilizados em casa utiliza este protocolo para atribuir os IPs aos computadores da rede.

Nota: Este protocolo é o sucessor do BOOTP que, embora mais simples, se tornou limitado para as exigências atuais.

O DHCP usa um modelo cliente-servidor, no qual o servidor DHCP mantém a gestão centralizada dos endereços IP usados na rede.

Resumidamente, o DHCP opera da seguinte forma:

- Um cliente envia um pacote UDP em *broadcast* (destinado a todas as máquinas) com um pedido DHCP
- Os servidores DHCP que capturarem este pacote irão responder (se o cliente se enquadrar numa série de critérios — ver abaixo) com um pacote de configurações onde constará, pelo menos, um endereço IP, uma máscara de rede e outros dados opcionais, como o gateway, servidores de DNS, etc.

Critérios de atribuição de IPs

O DHCP oferece três tipos de atribuição (alocação) de endereços IP:

- **Atribuição manual** - Onde existe uma tabela de associação entre o Endereço MAC do cliente (que será comparado através do pacote *broadcast* recebido) e o endereço IP (e restantes dados) a fornecer. Esta associação é feita manualmente pelo administrador de rede; por conseguinte, apenas os clientes cujo MAC consta nesta lista poderão receber configurações desse servidor
- **Atribuição automática** - Onde o cliente obtém um endereço de um espaço de endereços possíveis, especificado pelo administrador. Geralmente qualquer endereço MAC é aceite
- **Atribuição dinâmica** - O único método que dispõe a reutilização dinâmica dos endereços. O administrador disponibiliza um espaço de endereços possíveis, e cada cliente terá o software TCP/IP da sua interface de rede (placa de rede) configurados para requisitar um endereço por DHCP assim que a máquina arranque. A alocação utiliza um mecanismo de *aluguer* do endereço, caracterizado por um tempo de vida. Após a máquina se desligar, o tempo de vida naturalmente irá expirar, e da próxima vez que o cliente se ligue, o endereço provavelmente será outro (isto acontece, por exemplo, nas nossas ligações à Internet, em que um dia podemos ter um certo endereço público mas no dia seguinte já teremos outro)

DNS

Domain Name System (Sistema de Nomes de Domínios) é um sistema de gestão de nomes que tem a função de traduzir os endereços escritos “por palavras” em endereços IP escritos em números. Ou seja, os servidores DNS, contêm listas de endereços onde os nomes estão relacionados com endereços IP. Funcionam como uma espécie de Páginas Amarelas gigante, com os endereços de todos os servidores existentes (ou, então, estão ligados a outros servidores com outras listas).

Por exemplo, ao escrevermos www.google.com no *browser*, o nosso “pedido” vai para um servidor DNS, que procura na sua lista o IP correspondente (por exemplo, 64.68.92.29) e o devolve ao nosso *browser*. A partir daí, o browser automaticamente se liga a esse endereço.

Normalmente, ao configurar uma rede/host é necessário definir o endereço IP do servidor DNS. Se este não for automaticamente atribuído por DHCP, então, teremos de saber esse endereço. Uma vez mais, na nossa rede doméstica, poderemos perguntar ao fornecedor de Internet quais os endereços dos seus servidores DNS para configurarmos a nossa rede.

Algumas ferramentas (em Windows)

Em Windows, podemos utilizar algumas ferramentas em linha de comando para ajudar a configurar uma rede local e verificar se está tudo a funcionar correctamente.

Para aceder à linha de comandos (em Windows XP), ir ao botão “Iniciar”, seleccionar “Executar” e escrever o comando “cmd”. A partir daí surge uma janela onde podemos escrever alguns comandos:

ping – serve para verificar a ligação a um endereço; se houver uma máquina disponível com o endereço que escrevemos, então ela responde; caso não haja, obtemos “O pedido excedeu o tempo”.

Utilização:

ping 192.168.1.10

ping www.google.pt

tracert – serve para verificar a rota que segue um pedido de um endereço; isto é, com este comando podemos verificar todos os “saltos” que o nosso pedido dá, ao passar de um host para outro, até chegar ao endereço que escrevemos

Utilização

tracert 192.168.1.10

tracert www.youtube.com

ipconfig – serve para verificar, renovar e configurar os vários endereços de um adaptador de rede (placa de rede); ao utilizarmos este comando, podemos ver a configuração de um ou mais adaptadores de rede no nosso host

Utilização

ipconfig ← simples; mostra o nome (usado pelo DNS) que identifica a ligação, o endereço IP, a máscara de sub-rede e o endereço DNS

ipconfig /all ← além das definições descritas acima, mostra outras definições

ipconfig /release ← para “libertar” os endereços atribuídos

ipconfig /renew ← para renovar os endereços (caso seja automático, envia um novo pedido ao servidor DHCP)

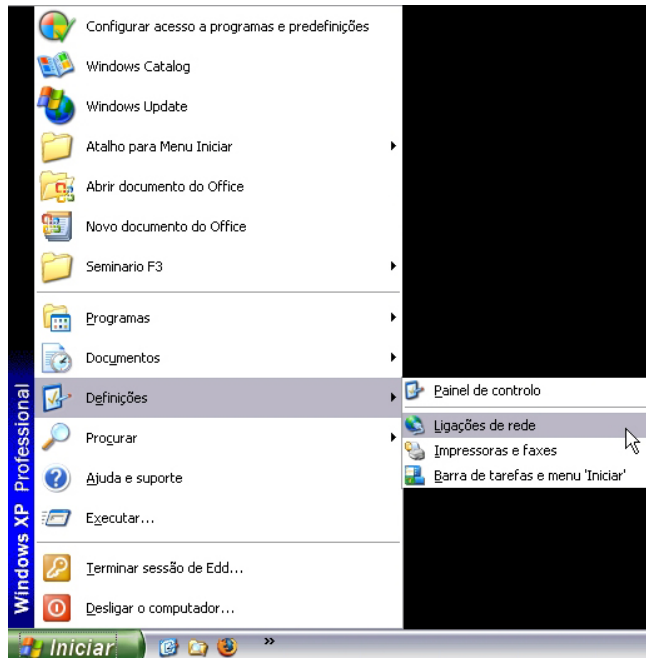
É possível ver as definições de apenas um adaptador de rede, baseado no seu nome, ou mesmo um conjunto de adaptadores de rede, bem como outras informações. Para ver todas as opções, escrever: **ipconfig /h**

Configuração de uma Ligação de Área Local em ambiente Windows (XP)

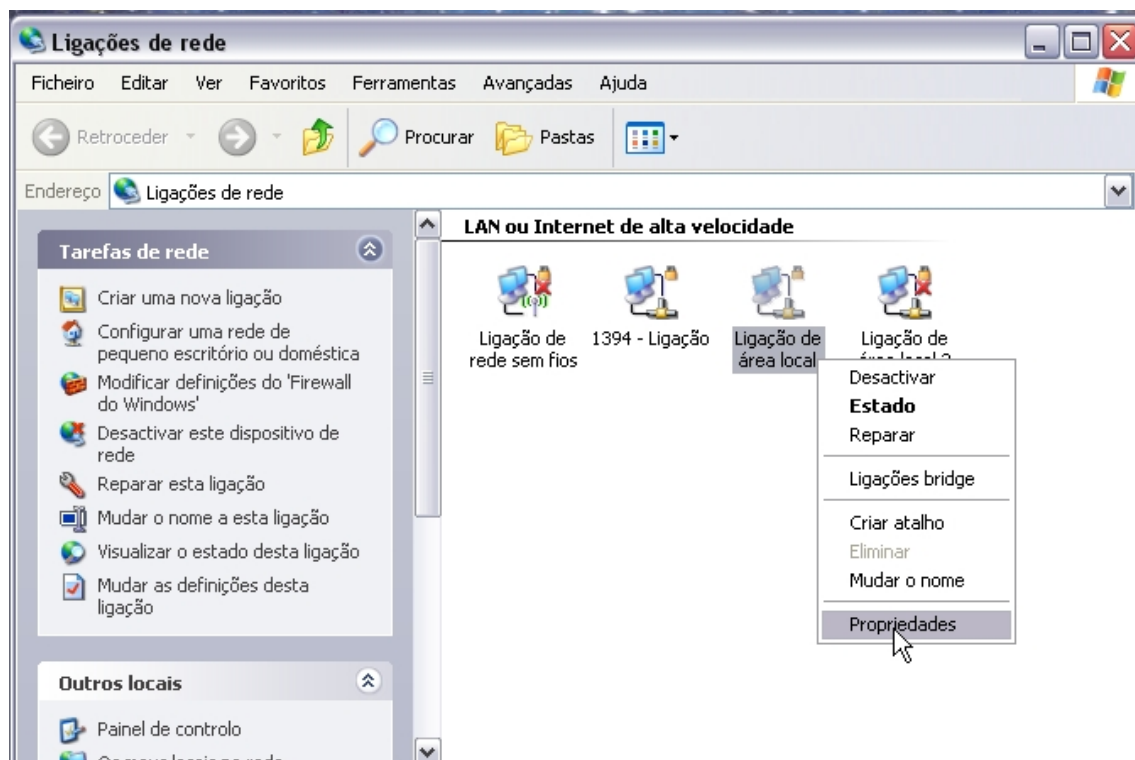
Botão “Iniciar” → “Ligações de rede”

ou

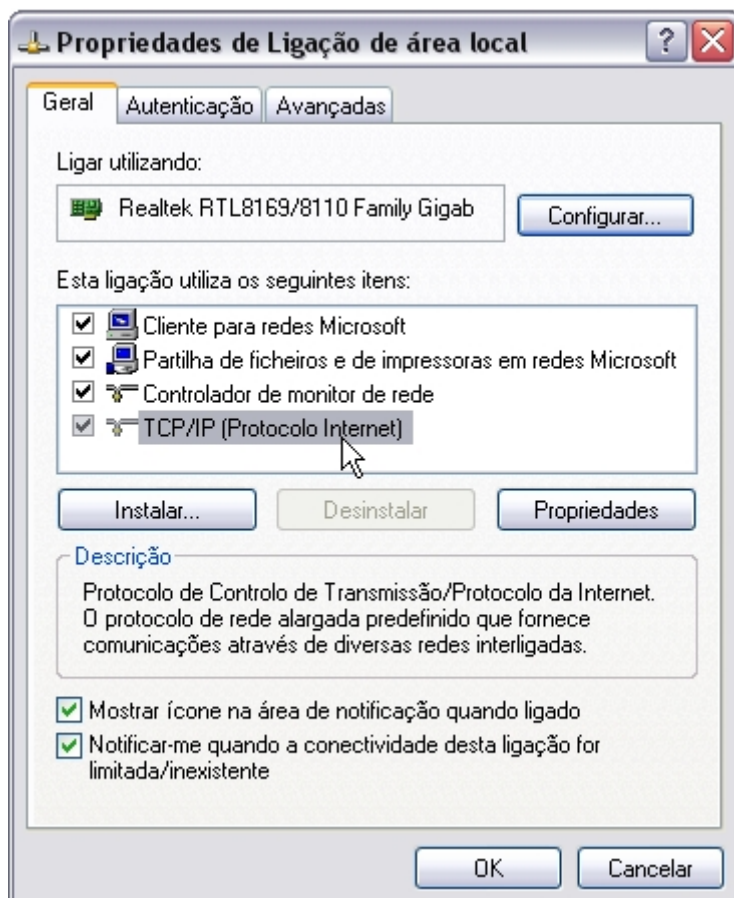
Botão “Iniciar” → “Painel de Controlo” → “Ligações de Rede”



Na janela “Ligações de Rede”, utilizar o botão direito do rato na ligação que queremos configurar e seleccionar “Propriedades”



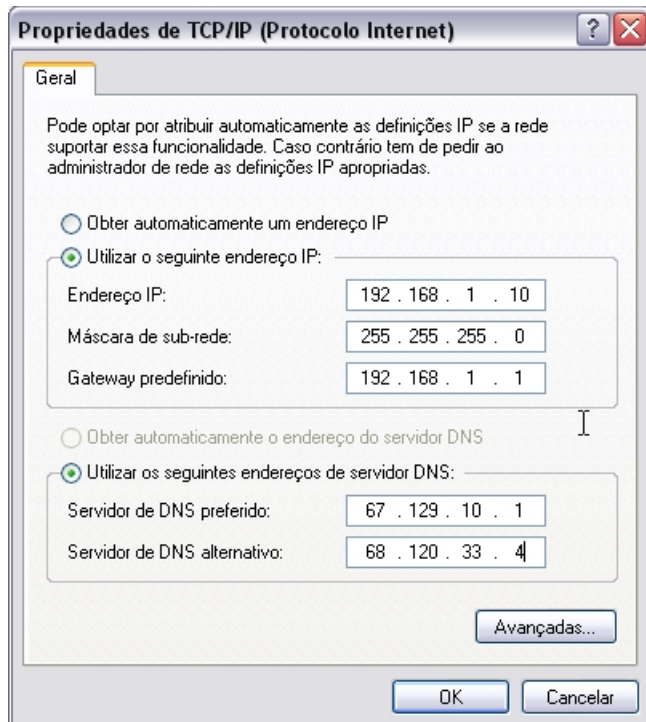
Na janela que surge, seleccionar o item “TCP/IP (Protocolo Internet)” e clicar OK (ou duas vezes com o rato)



Isto abre a janela de configuração de TCP/IP.

Aqui, podemos configurar

Endereços estáticos - endereços IP/máscara de sub-rede, gateway e DNS estáticos (definido pelo utilizador/administrador)



Endereços dinâmicos/automáticos - endereços IP/máscara de sub-rede, gateway e DNS automáticos (atribuídos pelo servidor DHCP)

