

Protocolos da Camada de Rede	52
IP (Internet Protocol)	52
ARP	54
ICMP	56
IGMP	57
Protocolos da Camada de Transporte	58
TCP (Transmission Control Protocol)	58
UDP (User Datagram Protocol)	59
Protocolos da Camada de Aplicação / APIs	60
Arquitetura Cliente-Servidor	60
RPC	61
Portas	62
Sockets	63
NetBIOS	64
Protocolos da Camada de Aplicação / Suporte	65
Resolução de nomes de domínio (DNS)	65
WINS	70
DHCP	73
RARP	78
BOOTP	78
SNMP	79
RMON	82
Protocolos da Camada de Aplicação / Usuário	83
HTTP (HyperText Transfer Protocol)	83
SMTP	84
POP3	85
IMAP4	86
NNTP	87
LDAP	88
NFS	89
FTP	90
Telnet	91
Utilitários TCP/IP	92
Arp	92
Ftp	93
Ipconfig	96
Nbtstat	97
Netstat	98
Nslookup	99
Ping	103
Utilitários Remotos do BSD Unix	106
Route	108
Telnet	110
Tftp (Trivial File Transfer Protocol)	111
Tracert (traceroute no Unix)	112
Apêndice	113
Domínios de primeiro nível no Brasil (DNS)	113
Códigos de países utilizadas no DNS	114
Portas TCP/UDP Padronizadas	116
Notação Binária	118
Conclusão	119
Estrutura do Cabeçalho IP	120
Estrutura do Cabeçalho TCP	122
Estrutura do Cabeçalho UDP	124
Informações Adicionais	125
Índice	126

Ilustrações

Eleida Pereira de Camargo e Luciano Palma

O que é um Protocolo de Rede

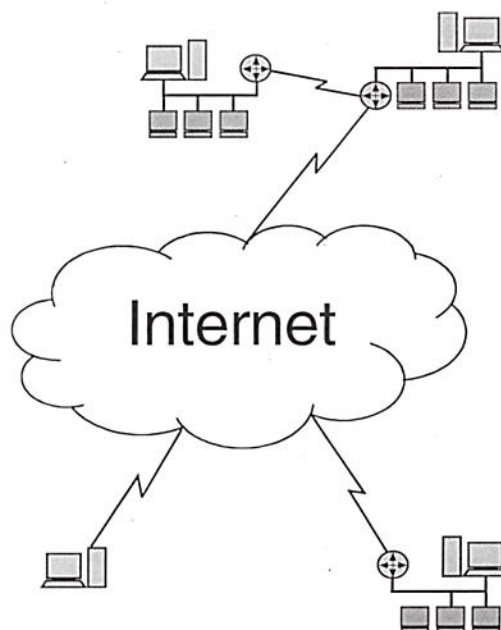
Protocolo de rede é um conjunto de regras utilizadas pelos computadores de uma rede para estabelecer a comunicação entre eles. Assim como na linguagem falada, onde duas pessoas somente se comunicam se falarem a mesma língua, dois computadores só podem se comunicar se utilizarem o mesmo protocolo.

O que é o Protocolo TCP/IP

TCP/IP é um conjunto de protocolos usados em redes de computadores. TCP e IP são dois protocolos dessa família e por serem os mais conhecidos, tornou-se comum usar o termo TCP/IP para se referir à família inteira. É também usual falar em "suite TCP/IP" para designar um pacote contendo o protocolo TCP/IP e alguns utilitários auxiliares.

O protocolo TCP/IP permite a conexão de computadores tanto em pequenas redes locais (LAN) quanto em redes corporativas interligando diversos países (WAN). O maior exemplo disso é a própria Internet, que adota o protocolo TCP/IP.

Todos os sistemas operacionais atuais (Windows, Linux, Unix, MacOS, Netware, etc) fornecem uma implementação do protocolo TCP/IP.



Padrão x Implementação

Um dos objetivos do TCP/IP é estabelecer um padrão para que computadores de fabricantes distintos se comuniquem.

Esse padrão consiste na **definição** de como acontecerá a comunicação, estabelecendo regras que norteiam o envio e o recebimento dos dados. Padrões são normalmente discutidos e definidos por organizações independentes.

Cada fabricante desenvolve seus programas de comunicação, de acordo com o que estipula o padrão. Diz-se então que o fabricante **implementa** o padrão, ou seja, o software TCP/IP que acompanha o Windows é a **implementação** da Microsoft do **padrão** TCP/IP. Da mesma maneira, o Solaris traz a implementação da Sun, o AIX traz a implementação da IBM, o IntraNetware traz a implementação da Novell, etc.

É possível, portanto, encontrar pequenas diferenças entre as implementações de fabricantes distintos, seja em termos de desempenho ou de funcionalidade, uma vez que algumas regras do padrão podem ser de implementação opcional.

Neste guia os autores seguiram o padrão TCP/IP, sem discutir particularidades de uma implementação específica.

Nos exemplos deste guia foi utilizada a implementação da Microsoft, o que não implica em nenhuma preferência ou recomendação. Os leitores que utilizem outras implementações, tais como Linux, Netware ou qualquer versão de Unix, não terão dificuldades em entender os exemplos.

Como surgiu o TCP/IP

O desenvolvimento do protocolo TCP/IP começou em 1969, com o projeto ARPANET, da Agência de Projetos de Pesquisas Avançadas do Departamento de Defesa dos EUA (*Department of Defense Advanced Research Projects Agency - DARPA*).

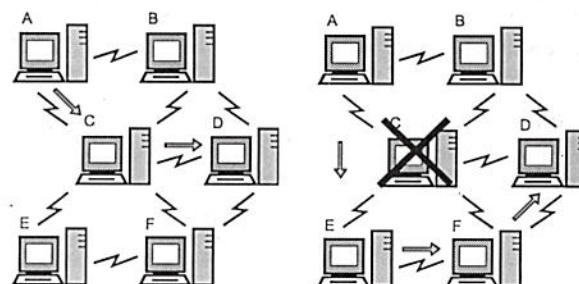
O objetivo desse projeto foi desenvolver uma rede que interligasse os computadores do governo americano, de diferentes fabricantes e utilizando diferentes sistemas operacionais. Essa rede deveria ser descentralizada e mesmo que um dos computadores dessa rede fosse destruído num eventual ataque militar, os demais continuariam a funcionar normalmente, graças a um mecanismo de rotas alternativas.

Algum tempo depois desse início com finalidade militar, a *National Science Foundation* criou uma rede semelhante para interconectar instituições de pesquisa e universidades, utilizando os mesmos protocolos da rede ARPANET.

Desses projetos surgiu o protocolo TCP/IP, que serviu como alicerce para a construção da rede que hoje conhecemos como *Internet*.

A partir de 1993 a Internet ficou disponível para uso comercial e se popularizou de tal forma, que hoje a maioria de nós a utiliza com familiaridade.

Rotas alternativas: A comunicação entre A e D não é interrompida pela falha do computador C graças à rota alternativa passando por E e F



Cronologia do Protocolo TCP/IP

Relacionamos abaixo alguns eventos significativos da evolução do protocolo TCP/IP e da Internet.

Ano	Evento
1969	ARPANET autorizada pelo DOD
1970	ARPANET adota o <i>Network Control Protocol</i> (NCP)
1971	23 hosts na ARPANET
1972	Especificação do <i>Telnet</i>
1973	Especificação do <i>File Transfer Protocol</i> (FTP)
1974	Especificação do <i>Transmission Control Protocol</i> (TCP)
1975	Primeiro <i>mailing list</i> da ARPANET (MsgGroup)
1978	TCP subdividido em TCP e IP
1981	Publicação do <i>Standard Internet Protocol</i> (IP)
1982	TCP e IP definidos como <i>suite</i> pela ARPA e DCA
1983	Substituição do NCT pelo TCP/IP (flag day)
1984	Surgimento do DNS1986: Criação da NFSNet
1986	Criação da IETF e da IRTF pela IAB
1987	10.000 hosts na NFSNet
1989	100.000 hosts na NFSNet
1990	ARPANET deixa de existir Brasil se conecta à NFSNet
1992	Criação da ISOC
1993	Criação do InterNIC
1994	Início do uso comercial da Internet no Brasil
1996	Guerra dos browsers: Microsoft x Netscape
1999	60.000.000 de hosts na Internet

Informações adicionais sobre o histórico da Internet podem ser obtidas no RFC 1120.

Quem é responsável pelo TCP/IP

TCP/IP é o protocolo utilizado na Internet e, embora nenhuma organização seja proprietária da Internet, a Internet Society (ISOC), uma entidade internacional não-governamental, coordena o desenvolvimento de novas tecnologias e aplicações da Internet. Essa entidade é composta por diversos membros (pessoas, empresas, agências governamentais e fundações) que participam desde a criação da Internet e têm colaborado ativamente no desenvolvimento de novas tecnologias para a Internet.

A ISOC possui um grupo consultivo conhecido como Internet Architecture Board (IAB), que coordena o funcionamento da Internet, bem como a pesquisa e o desenvolvimento relacionados com o funcionamento da Internet. O IAB tem as seguintes atribuições:

- A padronização dos protocolos da Internet, consequentemente do protocolo TCP/IP.
- A administração dos documentos RFC (Request For Comments).
- A coordenação das operações da IETF e da IRTF.
- O planejamento estratégico da Internet.

O IAB, por sua vez, é subdividido nos seguintes grupos:

- IETF (Internet Engineering Task Force), comunidade organizada em grupos de trabalho, responsável pelo desenvolvimento de soluções técnicas para os problemas que surgem na Internet e pela definição de padrões e protocolos para o funcionamento da Internet.
- IRTF (Internet Research Task Force), semelhante ao IETF, porém para pesquisas a longo prazo referentes ao funcionamento da Internet.
- IANA (Internet Assigned Numbers Authority), controla a distribuição de identificadores para serviços a serem fornecidos via Internet, tais como atribuição de endereços IP e números de porta TCP e UDP (ver páginas 116 e 117).

Qualquer membro da ISOC pode apresentar ao IAB uma proposta de padronização do TCP/IP, através de um documento chamado RFC (*Request For Comments*).

Informações adicionais sobre essas entidades podem ser obtidas em seus respectivos sites:

www.isoc.org, www.iab.org, www.ietf.org, www.irtf.org e www.iana.org.

RFCs (Requests For Comments)

A maior parte da documentação oficial sobre o protocolo TCP/IP está disponível através de uma série de documentos chamados RFCs (*Request For Comments*), que fornecem a base técnica para quem deseja um conhecimento mais profundo do TCP/IP.

Os padrões do protocolo TCP/IP não são desenvolvidos por um comitê. Qualquer membro da Internet Society (ISOC) pode elaborar e submeter um documento para análise e eventual publicação como RFC.

Cada documento RFC recebe a seguinte classificação:

Classificação	Significado
Necessário	RFC deve ser implementado.
Recomendado	RFC de uso bastante provável; é recomendada a sua implementação.
Opcional	RFC utilizado em alguns casos. Fica à critério da empresa implementá-lo ou não.
Uso limitado	RFC utilizado em condições muito específicas. Deve ser implementado somente nesses casos.
Não recomendado	RFC utilizado em condições excepcionais. Recomenda-se que não seja implementado.

Quando um documento RFC é publicado, ele recebe um número. Uma vez que isso acontece, o RFC nunca é alterado. Quando um RFC é revisado, um novo RFC é criado, recebendo um novo número, e o RFC anterior torna-se obsoleto.

Quando estiver pesquisando um tópico certifique-se de ter o RFC mais recente sobre o tópico.

Um RFC é publicado com o objetivo de se tornar um Standard (STD), que é uma padronização definitiva e com uma numeração distinta. Muitas vezes, porém, RFCs são utilizados como padrões de mercado, sendo implementados mesmo antes de se tornarem Standards.

Informações adicionais sobre RFCs podem ser obtidas nos seguintes sites:

- <http://www.rfc-editor.org/rfc.html>
Repositório das RFCs oficiais e definitivas.
- <http://www.faqs.org/rfcs/>
Informações sobre RFCs.

Modelos de Camadas

Para descrever a arquitetura do conjunto de protocolos TCP/IP geralmente é utilizado um modelo conceitual de camadas.

Cada camada do modelo define funções que um determinado componente de software ou hardware deve realizar. Para cada uma das camadas são desenvolvidos padrões que devem ser seguidos pelos fabricantes para garantir a compatibilidade com componentes de outros fabricantes.

O software que implementa cada uma dessas camadas é responsável por uma determinada função no processo de transmissão e recepção de dados.

Existem dois modelos: o modelo DARPA de 4 camadas e o modelo OSI de 7 camadas da ISO (International Standards Organization).

O modelo DARPA foi adotado desde o início do desenvolvimento do TCP/IP pois o modelo OSI ainda não tinha sido publicado, o que ocorreu somente em 1984, quando o TCP/IP já era um padrão consolidado.

Apesar das pressões do governo americano para a adoção do modelo OSI, o padrão DARPA continua sendo utilizado para descrever o protocolo TCP/IP e é o modelo que utilizaremos neste guia.

Cada camada no modelo DARPA corresponde aproximadamente a uma ou mais camadas no modelo de 7 camadas da OSI, porém não existe uma equivalência exata entre um modelo e outro, pois o TCP/IP é oficialmente independente do modelo OSI.

OSI	DARPA
Aplicação	Aplicação
Apresentação	
Sessão	Transporte
Transporte	
Rede	Interface de Rede
Enlace	
Física	

Unidades de Informação

Um conceito importante na comunicação de dados é o *empacotamento* da informação. Uma mensagem ou um arquivo não são transmitidos de uma única vez na rede. Eles são divididos em *unidades de informação (pacotes)*, normalmente de tamanho definido, e transmitidos aos poucos. O computador que envia as informações é responsável por essa divisão e o computador que as recebe é responsável por recompor a mensagem ou o arquivo no seu formato original. Essa técnica traz algumas vantagens:

- Se um pacote for corrompido ou perdido durante a transmissão de um arquivo, só aquele pacote deverá ser retransmitido, e não o arquivo todo.
- Se dois arquivos forem transmitidos simultaneamente numa mesma conexão, pacotes do primeiro e do segundo arquivos serão transmitidos alternadamente. Devido à alta velocidade dos equipamentos de rede atuais, verifica-se a transmissão "simultânea" dos arquivos.

As unidades de informação que cada camada da rede utiliza são diferentes, recebendo nomes distintos: mensagem, segmento, pacote, datagrama, frame, etc.

Muitas vezes essa miscelânea de termos gera confusões ou usos indevidos. O termo pacote, por exemplo, é utilizado indiscriminadamente entre os profissionais da área para designar unidades de informação de qualquer camada.

Terminologia das Unidades de Informação

Mensagem

Unidade de informação que a Camada de Aplicação passa para a Camada de Transporte.

Segmento

Unidade de informação utilizada pela Camada de Transporte.

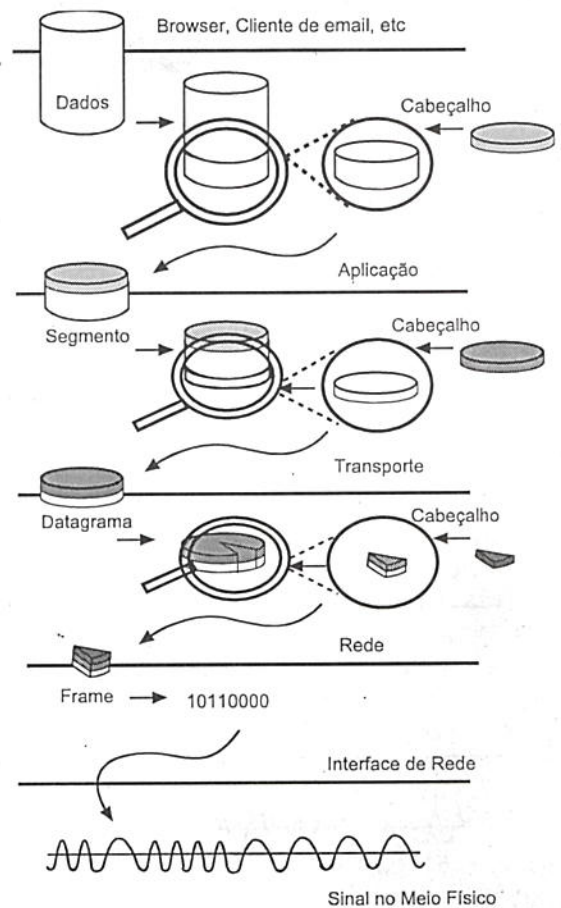
Datagrama

Unidade de informação que a Camada de Transporte passa para a Camada de Rede.

Frame

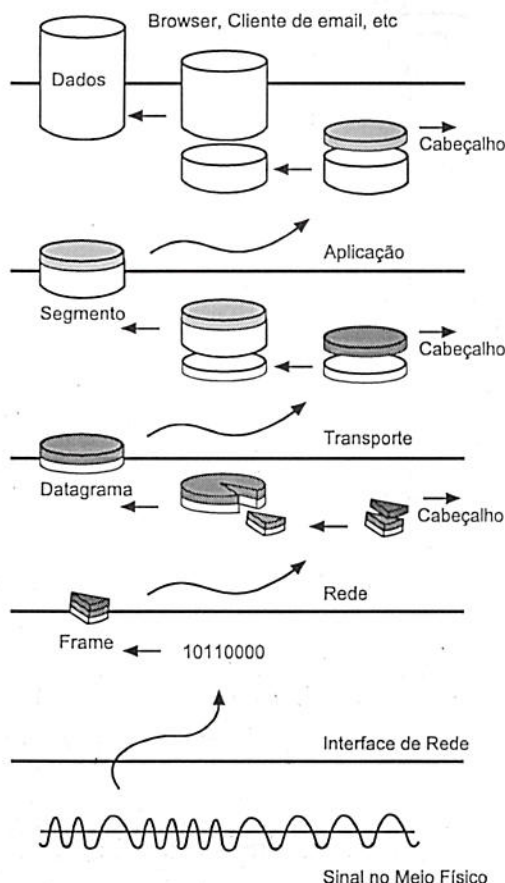
Unidade de informação que a Camada Interface de Rede utiliza para transmitir através do meio físico os dados recebidos da Camada de Rede.

Transmissão de Dados nas Camadas



1. Dados da camada de aplicação são passados para a camada de transporte, que os divide em segmentos adicionando o cabeçalho da camada de transporte (TCP ou UDP).
2. A camada de Transporte passa os dados para a camada de Rede, subdividindo-os em datagramas.
3. A camada de Rede adiciona seu cabeçalho (IP) aos dados e passa-os para a camada de Interface de Rede, subdivididos em frames.
4. A camada de Interface de Rede adiciona seu cabeçalho ao frame e transforma os dados em sinal elétrico para enviá-los através do meio físico.

Recepção de Dados nas Camadas



1. O sinal do meio físico dá origem a um frame na camada de Interface de Rede. Essa camada interpreta o cabeçalho do frame e retira-o, passando somente os dados do frame para a camada de Rede.
2. A camada de Rede agrupa diversos frames que compõem um datagrama, analisa o cabeçalho da camada de rede (IP) e passa somente os dados do datagrama para a camada de Transporte (descartando o cabeçalho IP)
3. Os datagramas são agrupados, formando um segmento na camada de Transporte. Essa camada analisa o cabeçalho (TCP ou UDP) e passa os dados (sem o cabeçalho) para a camada de aplicação, que finalmente recompõe os dados originalmente enviados pelo computador de origem.

Camada de Aplicação (Application)

Esta camada permite que aplicações tenham acesso às camadas inferiores através de portas TCP e UDP e define os protocolos utilizados por essas aplicações para envio e recepção de dados.

Para facilitar o entendimento da variedade de protocolos da camada de Aplicação, subdividimos essa camada em três grupos:

Interfaces de programação (APIs)

As APIs definem funções que permitem aos programadores desenvolver aplicações que acessem recursos de rede. As principais APIs utilizadas em redes TCP/IP são Sockets e NetBIOS. Para mais detalhes veja as páginas 60 a 64.

Serviços de suporte às operações de rede

São utilizados de forma indireta pelos usuários. Por exemplo, um usuário que acesse o site www.novatecl.com estará se utilizando do serviço DNS para descobrir o endereço IP relativo a esse nome.

Os principais serviços de suporte às operações de rede são: DNS, WINS, DHCP, BOOTP, SNMP e RMON. Esses serviços são descritos em detalhes a partir da página 65.

Serviços direcionados ao usuário final

Estes serviços são utilizados diretamente pelos usuários finais. Os principais serviços são: HTTP, SMTP, POP, NNTP, TELNET, FTP e TFTP.

Esses serviços são descritos em detalhes a partir da página 83.

Aplicação
Transporte
Rede
Interface de Rede

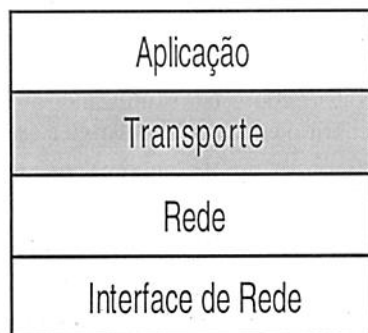
Camada de Transporte (Transport)

Os protocolos da camada de transporte coordenam o envio de mensagens de um computador a outro, podendo ou não implementar algum mecanismo de controle para garantir a entrega das mensagens.

Esses protocolos recebem pacotes da Camada de Aplicação e dividem-nos em *segmentos*, que são passados para a Camada de Rede.

Protocolo	Descrição
TCP	Protocolo <i>com conexão</i> e com garantia de entrega do pacote.
UDP	Protocolo <i>sem conexão</i> e sem garantia de entrega do pacote.

Esses serviços são descritos nas páginas 58 e 59.



Camada de Rede (Internet)

A Camada de Rede define o mecanismo utilizado para que o computador de origem localize o computador de destino, definindo a rota que as mensagens deverão percorrer.

Os protocolos da Camada de Rede recebem datagramas da Camada de Transporte e analisam-nos para definir a rota que será utilizada.

Nessa camada residem quatro protocolos (ARP, ICMP, IGMP e IP), que passam os datagramas recebidos da Camada de Transporte, adicionados ao cabeçalho IP, para a Camada de Interface de Rede.

Protocolo	Descrição
IP	Define os mecanismos de endereçamento e roteamento de pacotes na rede.
ARP	Fornece o endereço de hardware para hosts localizados na mesma rede física.
ICMP	Fornece informações sobre as condições de transmissão de datagramas na rede ou sobre erros.
IGMP	Utilizado para especificar quais computadores pertencem a um <i>grupo multicast</i> .

Esses protocolos são descritos nas páginas 52 a 57.



Camada de Interface de Rede (Network Interface)

A Camada de Interface de Rede define os padrões de transmissão de informações através do meio físico. Está intimamente relacionada ao hardware e a maioria dos protocolos dessa camada é implementada pelos *device drivers* da placa de rede.

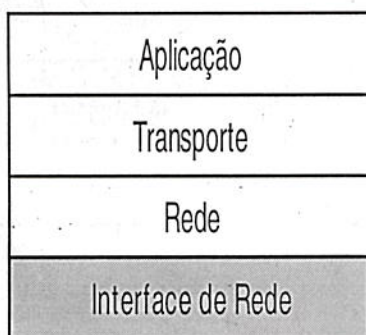
Os datagramas recebidos da Camada de Rede são subdivididos em *frames* e convertidos em sinal (elétrico, óptico, etc), para serem inseridos no meio físico de acordo com o tipo de rede:

Tipo de rede	Protocolo
Redes WAN	ATM, FDDI, Frame Relay e X.25
Redes LAN	Ethernet, Fast Ethernet, Token Ring e FDDI
Acesso Discado	PPP e SLIP

Na recepção de sinais vindos do meio físico (gerados por outro computador), os frames são reunidos, recompondo o datagrama original, que é transmitido para a Camada de Rede.

O tamanho do frame varia de um tipo de rede para outro, mas como a divisão é realizada pela Camada de Interface de Rede, a camada superior (rede) não precisa levar esse fator em consideração.

Os protocolos da camada de Interface de Rede são discutidos na página 51.



Conceitos Básicos de Endereçamento

Uma rede é um conjunto de computadores interligados através de algum meio físico (cabos, fibra ótica, etc) e com algum software instalado que permita a troca de informações entre eles. Cada computador é um *nó* da rede, denominado *host*.

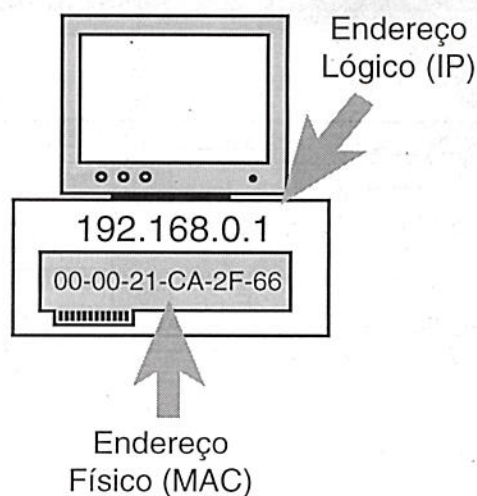
Os demais componentes da rede, como roteadores, *bridges* ou impressoras de rede também são denominados *hosts*.

Assim como numa rede telefônica, onde cada telefone tem um número para receber chamadas, as placas de rede dos computadores são identificadas através de um número: o *endereço físico*. O próprio fabricante atribui um endereço distinto a cada placa, garantindo que não existam duas placas com o mesmo endereço.

Utilizar diretamente os endereços físicos, porém, pode ser inconveniente. Imagine, por exemplo, ter que trocar de número de telefone caso seu aparelho apresente um defeito e deva ser substituído - o que pode acontecer com uma placa de rede. Por isso, a cada host é atribuído um *endereço lógico*, ou seja, um endereço que identifica aquele computador, independentemente da placa de rede que esteja usando. É claro que haverá sempre uma associação entre o endereço físico e o lógico, mas o software de rede se encarregará disso.

Diversas nomenclaturas são encontradas na literatura técnica, referindo-se ao endereço físico como *endereço Ethernet*, *endereço da placa de rede* ou *endereço MAC*, e ao endereço lógico como *endereço de rede* ou *endereço IP*.

Neste Guia, adotaremos os termos *endereço MAC* e *endereço IP*.



Endereço MAC

Cada dispositivo de rede recebe, de fábrica, um endereço "universalmente único", que é gravado em uma memória PROM do dispositivo. Esse endereço é denominado **endereço MAC**. Esse endereço é utilizado pelos protocolos da Camada de Interface de Rede (Ethernet, Token-Ring, FDDI, etc). É composto de 6 bytes, onde os 3 primeiros identificam o fabricante da placa (atribuídos pelo IEEE) e os 3 últimos são números únicos atribuídos pelo fabricante. Os bytes normalmente são exibidos em notação hexadecimal, separados por hífen, como por exemplo:

00-80-C7-E0-8E-B5, onde:

00-80-C7 Identifica o fabricante.

E0-8E-B5 Identifica o número de série.

É possível visualizar os endereços MAC das placas de rede instaladas em seu computador através do comando:

ipconfig /all

O endereço MAC é exibido na linha "Physical Address"

Exemplo:

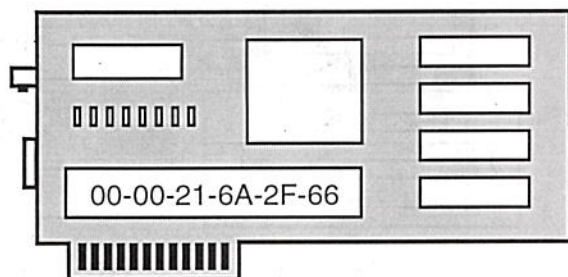
```

C:\>ipconfig /all

Ethernet adapter RTL80291:

Description . . . . . : Novell 2800 Adapter
Physical Address. . . . . : 00-00-21-6A-2F-66
DHCP Enabled. . . . . : No
IP Address. . . . . : 192.168.0.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
  
```

O endereço MAC é gravado na própria placa de rede:



Endereços de rede e endereços de host

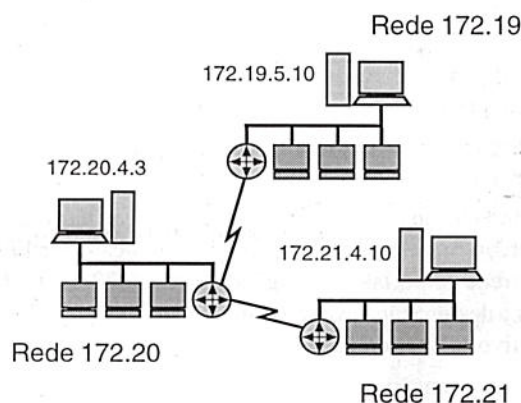
O protocolo TCP/IP permite integrar diversas redes, compondo uma internet. A palavra internet (com i minúsculo) refere-se a múltiplas redes conectadas através de roteadores (uma estrutura privada).

Internet (com I maiúsculo), por sua vez, refere-se à Internet pública, de abrangência mundial e que estamos habituados a utilizar.

A cada rede é atribuído um número, o **endereço de rede**. Cada host da rede recebe um número que o identifica dentro da sua rede: o **endereço de host**.

O endereço lógico é composto, no caso do TCP/IP, por duas partes: o **endereço de rede** e o **endereço de host**.

Voltando à analogia com a rede telefônica: o prefixo indica a região onde um telefone se encontra (endereço de rede) e o número do telefone (endereço lógico) é composto por esse prefixo e um identificador dentro da sua região (endereço de host).



Um termo muito utilizado atualmente (muitas vezes erroneamente) é **intranet**. Refere-se a uma rede de computadores (privada) que utilize os padrões da Internet na implementação de seus serviços (protocolo TCP/IP, distribuição de informação através de Web Servers / browsers, etc). Isto facilita a integração com redes de outras empresas (uma vez que os protocolos são os mesmos), utilizando até mesmo a própria Internet como base, criptografando os dados para garantir o sigilo das empresas (formando uma rede privada virtual, ou VPN – *Virtual Private Network*). Alguns autores denominam esta última como "extranet".

Endereço IP

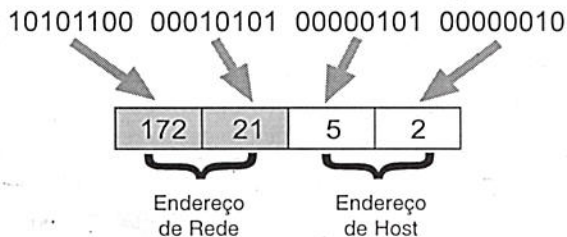
O protocolo responsável pelo roteamento e entrega dos pacotes de informação é o protocolo IP (camada de rede), portanto o endereço utilizado neste processo é designado **endereço IP**.

O endereço IP, portanto, deve conter a identificação da rede à qual o host pertence (endereço de rede) e o seu endereço dentro dessa rede (endereço de host).

O endereço de um host numa rede TCP/IP é composto de quatro bytes (32 bits), onde cada byte é representado em notação decimal. Os bytes são separados por pontos.

A representação de um endereço IP pode ser, por exemplo:

172.21.5.2



Parte desse endereço indica a rede à qual o *host* pertence e a outra parte identifica o *host* dentro da rede.

Nesse caso, a rede poderia ser definida pelos dois primeiros bytes e o host pelos dois últimos bytes.

Isso indica que todos os hosts da mesma rede têm o mesmo endereço de rede, ou seja, todos eles começam por 172.21. Essa rede é, portanto, designada a rede 172.21.0.0 (para obter a designação da rede, completa-se os bytes "faltantes" [relativos ao endereço de *host*] com zeros).

O host ao qual nosso exemplo se refere é o host 5.2 na rede 172.21.

Um administrador de rede deve garantir que não existam dois hosts utilizando o mesmo endereço IP em uma rede.

O endereço IP é definido nos RFCs 791, 1122 e 1812.

Computadores Multihomed

Hosts podem ser estações de trabalho, servidores, impressoras, roteadores, etc. Se um host tiver mais de uma placa de rede (NIC), cada placa deve ter seu próprio endereço IP.

Computadores que utilizam mais de um endereço IP são denominados computadores multihomed.

Endereços de rede privados

Cada país possui um órgão responsável pela atribuição de endereços IP às máquinas conectadas à Internet (no Brasil, esse órgão é a Embratel). Esse órgão deve garantir que um mesmo endereço IP não seja utilizado por mais de um host.

Algumas empresas, porém, implementaram suas redes privadas (Intranets) atribuindo indevidamente a seus hosts endereços IP já existentes na Internet, para evitar a burocracia e o alto custo de obter oficialmente esses endereços, ou ainda porque não planejavam conectar suas redes à Internet.

Foram reservados, então (através da RFC 1627), intervalos de endereços IP para serem utilizados exclusivamente em redes privadas. Esses endereços não devem ser roteados para a Internet. Mesmo que isso ocorra, os roteadores que compõem o *backbone* da Internet estão programados para desprezar pacotes originados por endereços reservados.

Os endereços reservados pela RFC 1627 são:

Classe	Intervalo de endereços
Classe A	10.0.0.0 até 10.255.255.255
Classe B	172.16.0.0 até 172.31.255.255
Classe C	192.168.0.0 até 192.168.255.255

Para mais detalhes sobre classes de endereços IP, veja a página 23.

Acesso à Internet

Um empresa que utilize endereços reservados (portanto não roteados para a Internet) pode ter acesso à Internet utilizando um Proxy ou através do recurso NAT.

Proxy

O Proxy possui duas placas de rede: uma conectada à rede privada, com um endereço IP reservado, e outra ligada à Internet, com um endereço válido na Internet. Sua função é similar à do roteador, encaminhando pacotes da rede interna para a Internet e vice-versa. O endereço IP interno (reservado) é substituído pelo endereço IP do Proxy (válido na Internet) para que os pacotes sejam roteados na Internet.