# OSI (Open Systems Interconnection)

Modelo criado pela ISO (International Organization of Standarization) em 1977, com o propósito de fornecer orientações sobre o funcionamento de sistemas de rede, tanto do ponto de vista do hardware como do software envolvido nesse sistema. Tal modelo é dividido em 7 camadas (layers) estratificando as funções dos diferentes componentes do sistema.

O modelo OSI não tem a função de definir uma implementação de sistema de rede específico, mas é um modelo conceitual que se presta como um guia conceitual para o desenvolvimento de sistemas específicos e seus protocolos (por exemplo a suíte de protocolos TCP/IP).

|  |  |
| --- | --- |
| Camadas no modelo OSI | Camadas implementadas na suíte TCP/IP |
| Aplicação | Aplicação (exemplo dos protocolos dessa camada: DHCP, DNS, FTP, HTTP, URL, IMAP, SMTP) |
| Apresentação |
| Sessão |
| Transporte | Transporte ( TCP UDP) |
| Rede | Internet (IP) |
| Link de Rede | Link (PPP PPTP L2TP) e interface de rede (ethernet, wi-fi) |
| Física |

fontes:

PENGELLY, James et al. The Official CompTIA Network+ Certification Self-Paced Study Guide (Exam N10-007). CompTIA, 2019.

<https://community.fs.com/blog/tcpip-vs-osi-whats-the-difference-between-the-two-models.html> - acesso em 20/09/2021

# TCP (Transmission Control Protocol)

Na estrutura conceitual dos modelos de redes (como o OSI ou o TCP/IP) o TCP é um protocolo da camada de transporte. Conforme coloca o RFC 761 (Request for Comments de 1981 que trata sobre o TCP) ele é um protocolo de conexão ponto a ponto que possibilita a comunicação segura entre processos em diferentes computadores.

Dentro da arquitetura de protocolos em camadas (como o OSI ou o TCP/IP) o TCP está imediatamente acima da camada de rede, essa, na arquitetura TCP/IP, é onde se situa o protocolo IP (Internet Protocol), do qual o TCP se vale para o envio e recebimento de informações por meio de pacotes chamados de datagramas de internet (internet datagrams).

fontes:

RFC 761:<https://datatracker.ietf.org/doc/html/rfc793#page-1> – acesso em 20/09/2021)

# TCP/IP (Transmission Control Protocol / Internet Protocol)

O TCP/IP é uma implementação específica de uma suíte de protocolos para o funcionamento de um sistema de redes (dizemos uma suíte de protocolos pois temos diversos protocolos cumprindo uma ou mais funções das diferentes camadas preconizadas para o sistema de rede). Enquanto o modelo OSI é um padrão técnico e conceitual, o modelo de TCP/IP é a implementação mais utilizada entre os sistemas de rede.

|  |  |
| --- | --- |
| Camadas no modelo OSI | Camadas implementadas na suíte TCP/IP |
| Aplicação | Aplicação (exemplo dos protocolos dessa camada: DHCP, DNS, FTP, HTTP, URL, IMAP, SMTP) |
| Apresentação |
| Sessão |
| Transporte | Transporte ( TCP UDP) |
| Rede | Internet (IP) |
| Link de Rede | Link (PPP PPTP L2TP) e interface de rede (ethernet, wi-fi) |
| Física |

fontes:

PENGELLY, James et al. The Official CompTIA Network+ Certification Self-Paced Study Guide (Exam N10-007). CompTIA, 2019.

<https://community.fs.com/blog/tcpip-vs-osi-whats-the-difference-between-the-two-models.html> - acesso em 20/09/2021

# UDP (User Datagram Protocol)

This protocol provides a procedure for application programs to send messages to other programs with a minimum of protocol mechanism. The protocol is transaction oriented, and delivery and duplicate protection are not guaranteed. Applications requiring ordered reliable delivery of streams of data should use the Transmission Control Protocol (TCP) [[2](https://datatracker.ietf.org/doc/html/rfc768#ref-2)].

Este protocolo providencia um procedimento para programas de aplicação enviarem mensagens para outros programas com o mínimo de mecanismo de protocolo. Esse protocolo é orientado à transação, e a proteção de duplicação de pacotes não é garantida. Aplicações que requerem um envio ordenado e confiável de uma corrente de dados devem usar o Protocolo de Controle de Transmissão (TCP) [[2](https://datatracker.ietf.org/doc/html/rfc768#ref-2)].

De <<https://datatracker.ietf.org/doc/html/rfc768>>

User Datagram Protocol (UDP), defined by **RFC 768** is a connectionless protocol. This protocol also operates at the Transport Layer of both the Open Systems Interconnection (OSI) reference model and the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol stack. However, unlike Transmission Control Protocol (TCP), the User Datagram Protocol (UDP) does not provide any guarantee or reassurance of the delivery of datagrams across a network. Not all protocols at the Application Layer uses TCP, there are many Layer 7 protocols which uses the User Datagram Protocol (UDP).

User Datagram Protocol (UDP), ou Protocolo de Datagrama de Usuário, definido pelo **RFC 768** é um protocolo sem conexão. Esse protocolo também opera na Camada de Transporte tanto da Open Systems Interconnection (OSI/Interconexão de Sistemas Abertos) modelo de referência e da pilha de protocolo TCP/IP. No entanto, diferente do Protocolo de Controle de Transmissão (TCP), o Protocolo de Datagrama de Usuário (UDP) não providencia asseguramento ou garantia da entrega de datagramas através de uma rede. Nem todos os protocolos da Camada de Aplicação usam o TCP, existem muitos protocolos de Camada 7 que se utilizam do Protocolo de Datagrama de Usuário (UDP).

De <<https://hub.packtpub.com/understanding-network-port-numbers-tcp-udp-and-icmp-on-an-operating-system/>>

# ICMP (Internet Control Message Protocol)

Internet Control Message Protocol (ICMP) defined by **RFC 792** is typically used to provide error reporting on a network. There are many types of Internet Control Message Protocol (ICMP) messages which provide different actions and give feedback if an error occurs, and also the issue which exists.

Protocolo de Mensagens de Controle(ICMP) definido pelo **RFC 792** é tipicamente utilizado para providenciar um relatório de erros de rede. Existem diversos tipos de mensagens de Protocolos de Mensagens de Controle (IMCP) onde cada uma providência diferentes ações que dão um parecer caso um erro aconteça, e qual o problema existente.

De <<https://hub.packtpub.com/understanding-network-port-numbers-tcp-udp-and-icmp-on-an-operating-system/>>

# Pacotes

É um termo que pode ter diferentes significados, de acordo com o contexto.

No contexto do protocolo TCP: é utilizado para referir a informação de uma transação que transita entre um host e sua rede (RFC793)

# Host

Literalmente pode ser traduzido como hospedeiro ou anfitrião. Muitas vezes é utilizado em contrapartida com o termo cliente, mas é um termo de acepção vinculada ao contexto de uso.

No contexto do protocolo TCP: se refere a um computador ligado a uma rede ou, de forma mais precisa, quando se referindo a perspectiva da comunicação na rede, pode ser a fonte de origem ou destino de pacotes. (RFC793)

# Processos

De forma muito genérica, um processo é um programa em execução. São os elementos ativos em um host. É, também um termo de acepção contextual.

No contexto do protocolo TCP: dizemos que toda a comunicação se dá entre processos. E a forma de distinção dos fluxos de comunicação de diferentes processos, nesse contexto, são as portas. (RFC793)

# Portas (Port)

No nível semântico, porta é um falso cognato utilizado para traduzir o termo port, do inglês, que literalmente seria traduzido por porto (de navios, local aonde chegam e de onde partem embarcações) (<https://pt.wikipedia.org/wiki/Porta_(inform%C3%A1tica)>).

De forma geral, na informática, dizemos que portas são pontos físicos ou lógicos de conexão. Podemos dizer que:

Portas físicas são as interfaces de um computador com periféricos externos ou mesmo entre as partes componentes do computador;

Portas lógicas são distinções lógicas, no nível dos programas, para diferentes pontos de troca de informações.

Mais uma vez temos que considerar usos contextuais, assim:

No contexto do protocolo TCP: portas são identificadores utilizados pelo protocolo para a distinção de diferentes fluxos de comunicação, originados por diferentes processos. O uso dos identificadores de portas, associados ao endereço IP (Internet Protocol) permite o estabelecimento e distinção de diversos fluxos de comunicação paralelos.

# Gateway

Em [telecomunicações](https://pt.wikipedia.org/wiki/Telecomunica%C3%A7%C3%B5es), o termo em inglês ***Gateway*** (em português ***Ponte de ligação***) refere-se a um pedaço de [hardware de rede](https://pt.wikipedia.org/wiki/Hardware_de_rede) que possui os seguintes significados:

* Em uma [rede de comunicações](https://pt.wikipedia.org/wiki/Rede_de_telecomunica%C3%A7%C3%B5es), um [nó](https://pt.wikipedia.org/wiki/N%C3%B3_(redes_de_comunica%C3%A7%C3%A3o)) de rede equipado para interfacear com outra rede que usa [protocolos](https://pt.wikipedia.org/wiki/Protocolo_(ci%C3%AAncia_da_computa%C3%A7%C3%A3o)) diferentes.
* Um *gateway* pode conter dispositivos como tradutores de protocolo, dispositivos de [comparação de impedância](https://pt.wikipedia.org/wiki/Adapta%C3%A7%C3%A3o_de_imped%C3%A2ncias), conversores de taxas, isoladores de [falhas](https://pt.wikipedia.org/wiki/Falha_(tecnologia)) ou tradutores de [sinais](https://pt.wikipedia.org/wiki/Sinaliza%C3%A7%C3%A3o_(telecomunica%C3%A7%C3%B5es)) quando necessário para fornecer [interoperabilidade](https://pt.wikipedia.org/wiki/Interoperabilidade) de [sistemas](https://pt.wikipedia.org/wiki/Sistemas).
* Um *gateway* de tradução / mapeamento de protocolo interconecta redes com diferentes tecnologias de protocolo de rede, por meio da realização de conversões de protocolos requeridas.
* Um [computador](https://pt.wikipedia.org/wiki/Computador) ou [programa de computador](https://pt.wikipedia.org/wiki/Programa_de_computador) configurado para realizar as tarefas de um *gateway*.

*Gateways*, também chamados de [conversores de protocolo](https://pt.wikipedia.org/w/index.php?title=Conversores_de_protocolo&action=edit&redlink=1), podem operar em qualquer camada de rede. As atividades de um gateway são mais complexas que aquelas do [roteador](https://pt.wikipedia.org/wiki/Roteador) ou [*switch*](https://pt.wikipedia.org/wiki/Switch), uma vez que se comunicam usando mais de um protocolo.

Os computadores dos usuários de [Internet](https://pt.wikipedia.org/wiki/Internet) e os computadores que servem páginas para usuários são nós de rede, uma vez que os nós que conectam as redes entre elas são *gateways*. Por exemplo, os computadores que controlam o tráfego entre redes de empresas ou os computadores usados pelos [provedores de serviço de internet](https://pt.wikipedia.org/wiki/Fornecedor_de_acesso_%C3%A0_internet) para conectar usuários à Internet são nós de *gateway*.

De <<https://pt.wikipedia.org/wiki/Gateway>>

# IP [address]

Um **Endereço de Protocolo da Internet** (**Endereço IP**), do inglês **Internet Protocol address** (IP address), é um rótulo numérico atribuído a cada dispositivo (computador, impressora, smartphone etc.) conectado a uma [rede de computadores](https://pt.wikipedia.org/wiki/Rede_de_computadores) que utiliza o [Protocolo de Internet](https://pt.wikipedia.org/wiki/Protocolo_de_Internet) para comunicação.[[1]](https://pt.wikipedia.org/wiki/Endere%C3%A7o_IP#cite_note-rfc760-1) Um endereço IP serve a duas funções principais: identificação de interface de hospedeiro ou de rede e [endereçamento](https://pt.wikipedia.org/wiki/Endere%C3%A7o_de_rede) de localização.

De <<https://pt.wikipedia.org/wiki/Endere%C3%A7o_IP>>

# IPV4

O [Protocolo de Internet versão 4](https://pt.wikipedia.org/wiki/IPv4) (IPv4) define um endereço IP como um número de [32 bits](https://pt.wikipedia.org/wiki/32_bits).[[1]](https://pt.wikipedia.org/wiki/Endere%C3%A7o_IP#cite_note-rfc760-1) Entretanto, devido ao crescimento da Internet e o [esgotamento de endereços IPv4 disponíveis](https://pt.wikipedia.org/wiki/Exaust%C3%A3o_do_IPv4), uma nova versão do IP ([IPv6](https://pt.wikipedia.org/wiki/IPv6)), usando 128 bits para o endereço IP, foi desenvolvida em 1995[[2]](https://pt.wikipedia.org/wiki/Endere%C3%A7o_IP#cite_note-rfc1883-2) e padronizada como [RFC 2460](https://tools.ietf.org/html/rfc2460) em 1998.[[3]](https://pt.wikipedia.org/wiki/Endere%C3%A7o_IP#cite_note-rfc2460-3) A implantação do IPv6 está em andamento desde meados de 2000.

De <<https://pt.wikipedia.org/wiki/Endere%C3%A7o_IP>>

# Network Address Translator (NAT)

Em [redes de computadores](https://pt.wikipedia.org/wiki/Redes_de_computadores), **Network Address Translation** (**NAT**), também conhecido como *masquerading*, é uma técnica que consiste em reescrever, utilizando-se de uma [tabela *hash*](https://pt.wikipedia.org/wiki/Tabela_hash)*,* os [endereços IP](https://pt.wikipedia.org/wiki/Endere%C3%A7o_IP) de origem de um pacote que passam por um [*router*](https://pt.wikipedia.org/wiki/Router) ou [*firewall*](https://pt.wikipedia.org/wiki/Firewall) de maneira que um [computador](https://pt.wikipedia.org/wiki/Computador) de uma [rede interna](https://pt.wikipedia.org/wiki/Rede_privada) tenha acesso ao exterior ou Rede Mundial de Computadores.[[1]](https://pt.wikipedia.org/wiki/Network_address_translation#cite_note-1)

Por se tratar de uma rede privada, os números de [IP](https://pt.wikipedia.org/wiki/IP) interno da rede (como 10.0.0.0/8, 172.16.0.0/12 e 192.168.0.0/16) nunca poderiam ser passados para a [Internet](https://pt.wikipedia.org/wiki/Internet) pois não são [roteados](https://pt.wikipedia.org/w/index.php?title=Rote%C3%A1veis&action=edit&redlink=1) nela e o computador que recebesse um pedido com um desses números não saberia para onde enviar a resposta. Sendo assim, os pedidos teriam de ser gerados com um IP global do router. Mas quando a resposta chegasse ao router, seria preciso saber a qual dos computadores presentes na LAN pertencia aquela resposta.

A solução encontrada foi fazer um mapeamento baseado no IP interno e na porta local do computador. Com esses dois dados o NAT gera um número de 16 [bits](https://pt.wikipedia.org/wiki/Bit) usando a [tabela hash](https://pt.wikipedia.org/wiki/Tabela_hash), este número é então escrito no campo da porta de origem.

De <<https://pt.wikipedia.org/wiki/Network_address_translation>>

# WhoIS

WHOIS é um serviço fornecido pela InterNIC que fornece informações sobre domínios de segundo nível, incluindo endereços de email de contato, endereços postais e números de telefone daqueles que se registraram no InterNIC. O WHOIS também pode ajudar a determinar se um nome de domínio já está em uso que pode ser útil para novos administradores de site.

O WHOIS pode ser acessado por meio de clientes WHOIS, sessões interativas de telnet, email e World Wide Web. O banco de dados InterNIC fornece informações sobre domínios COM, .EDU, .NET, .ORG e .GOV.

De <<https://docs.microsoft.com/pt-br/troubleshoot/windows-server/networking/research-internet-domains-with-whois>>

# DNS (Domain Name System)

O **Sistema de Nomes de Domínio,**[[1]](https://pt.wikipedia.org/wiki/Sistema_de_Nomes_de_Dom%C3%ADnio#cite_note-ICANN:0-1)[[2]](https://pt.wikipedia.org/wiki/Sistema_de_Nomes_de_Dom%C3%ADnio#cite_note-2)[[3]](https://pt.wikipedia.org/wiki/Sistema_de_Nomes_de_Dom%C3%ADnio#cite_note-3) mais conhecido pela nomenclatura em Inglês **Domain Name System** (**DNS**), é um sistema hierárquico e distribuído de gestão de nomes para computadores, serviços ou qualquer máquina conectada à [Internet](https://pt.wikipedia.org/wiki/Internet) ou a uma [rede privada](https://pt.wikipedia.org/wiki/Rede_privada). Faz a associação entre várias informações atribuídas a nomes de domínios e cada entidade participante. A sua utilização mais convencional associa nomes de domínios mais facilmente memorizáveis a [endereços IP](https://pt.wikipedia.org/wiki/Endere%C3%A7o_IP) numéricos, necessários à localização e identificação de serviços e dispositivos, processo esse denominado por: **resolução de nome**. O desempenho não se degrada substancialmente quando se adicionam mais servidores. Por padrão, o DNS usa o protocolo [User Datagram Protocol (UDP)](https://pt.wikipedia.org/wiki/User_Datagram_Protocol) na [porta](https://pt.wikipedia.org/wiki/Porta_(redes_de_computadores)) 53 para servir as solicitações e as requisições.[[4]](https://pt.wikipedia.org/wiki/Sistema_de_Nomes_de_Dom%C3%ADnio#cite_note-rfc1035-4)

De <<https://pt.wikipedia.org/wiki/Sistema_de_Nomes_de_Dom%C3%ADnio>>

# .br Registro.br e CGI.br

Criado e delegado ao [Brasil](https://pt.wikipedia.org/wiki/Brasil) em [1989](https://pt.wikipedia.org/wiki/1989)[[2]](https://pt.wikipedia.org/wiki/.br#cite_note-2) por [Jon Postel](https://pt.wikipedia.org/wiki/Jon_Postel),[[3]](https://pt.wikipedia.org/wiki/.br#cite_note-3) o domínio era, inicialmente, operado de forma manual pelo [Registro.br](https://pt.wikipedia.org/wiki/Registro.br) e administrado pela [Fundação de Amparo à Pesquisa do Estado de São Paulo](https://pt.wikipedia.org/wiki/Funda%C3%A7%C3%A3o_de_Amparo_%C3%A0_Pesquisa_do_Estado_de_S%C3%A3o_Paulo) (FAPESP). Essencialmente, apenas pesquisadores e as instituições às quais eles pertenciam tinham interesse e condições em se integrar à nova [rede](https://pt.wikipedia.org/wiki/Rede) e, portanto, em registrar um [domínio](https://pt.wikipedia.org/wiki/Dom%C3%ADnio) sob o .br.

Na época, as redes predominantes no cenário acadêmico brasileiro eram a [BITNET](https://pt.wikipedia.org/wiki/BITNET) (*Because It’s Time NETwork*), a [HEPnet](https://pt.wikipedia.org/wiki/HEPnet) (*High Energy Physics Network*) e a [UUCP](https://pt.wikipedia.org/wiki/UUCP) (*Unix-to-Unix Copy Program*). Assim, antes mesmo da [conexão](https://pt.wikipedia.org/wiki/Conex%C3%A3o) brasileira à [Internet](https://pt.wikipedia.org/wiki/Internet), que se daria em [1991](https://pt.wikipedia.org/wiki/1991), o domínio foi utilizado para identificar as [máquinas](https://pt.wikipedia.org/wiki/M%C3%A1quina) que participavam das redes já utilizadas pelos acadêmicos.

Em [1995](https://pt.wikipedia.org/wiki/1995), o [Comitê Gestor da Internet no Brasil](https://pt.wikipedia.org/wiki/Comit%C3%AA_Gestor_da_Internet_no_Brasil) (CGI.br) foi criado para, entre outros objetivos, coordenar a atribuição de endereços Internet ([IPs](https://pt.wikipedia.org/wiki/IP)) e o registro de nomes de domínios .br. O [DNS](https://pt.wikipedia.org/wiki/DNS) (*Domain Name System*) brasileiro que, em [1996](https://pt.wikipedia.org/wiki/1996), começava o ano com 851 domínios registrados, experimentava um crescimento vertiginoso com a chegada em massa de empresas, provedores e mídia à Internet. O sistema de registro foi automatizado em [1997](https://pt.wikipedia.org/wiki/1997) e contou com desenvolvimento interno de software aberto.

Em [2005](https://pt.wikipedia.org/wiki/2005), o CGI.br criou seu próprio braço executivo, o [Núcleo de Informação e Coordenação do Ponto BR](https://pt.wikipedia.org/wiki/N%C3%BAcleo_de_Informa%C3%A7%C3%A3o_e_Coordena%C3%A7%C3%A3o_do_Ponto_BR) (NIC.br),[[4]](https://pt.wikipedia.org/wiki/.br#cite_note-4) que exerce atualmente tanto a função administrativa quanto operacional dos registros.

De <<https://pt.wikipedia.org/wiki/.br>>

# nslookup

**nslookup** é uma ferramenta comum ao Windows e ao Linux e utilizada para se obter informações sobre registros de [DNS](https://pt.wikipedia.org/wiki/Sistema_de_Nomes_de_Dom%C3%ADnio) de um determinado [domínio](https://pt.wikipedia.org/wiki/Dom%C3%ADnio), [host](https://pt.wikipedia.org/wiki/Host) ou [ip](https://pt.wikipedia.org/wiki/Endere%C3%A7o_IP).

Ele pode trabalhar de duas formas: modo interativo ou não interativo

Modo interativo - o comando interage com vários servidores de domínios e com várias máquinas. O comando executa neste modo quando o primeiro argumento é o endereço ou o nome de um servidor de domínio do qual serão mostradas as informações.

Modo não interativo - o comando interage apenas com uma máquina específico. O comando entra nesse modo quando nenhum argumento de configuração é fornecido, ou quando o primeiro argumento é um sinal de menos (-) e o segundo argumento é o nome de uma máquina ou de um servidor de domínios.

Um conjunto de argumentos podem ser especificados no arquivo .nslookup, no diretório "home" do usuário.

De <<https://pt.wikipedia.org/wiki/Nslookup>>