

A origem da Internet

Há 40 anos, enquanto os principais **meios de comunicação** eram o telégrafo e o telefone, os computadores eram grandes máquinas que realizavam cálculos e armazenavam informações. De forma geral, seu uso tinha fins exclusivamente científicos e governamentais.

Então, como foi que chegamos à chamada **Era da Informação**, na qual a tecnologia invade todos os aspectos de nossas vidas? Se quisermos encontrar uma resposta para essa pergunta, precisamos retroceder na história da Internet.

Em 1957, os Estados Unidos e a União Soviética protagonizavam a Guerra Fria, um embate em termos ideológicos, econômicos, políticos, militares e, é claro, tecnológicos.

Devido ao conflito, os Estados Unidos estavam interessados em encontrar uma maneira de proteger suas informações e comunicações no caso de um ataque nuclear soviético. As **inovações** que tentaram resolver esse problema levaram ao que conhecemos hoje como Internet.

Primeiros conceitos e propósitos da Internet

Agora, falaremos sobre os primeiros acontecimentos que deram início à Internet:

DARPA

Em 1958, um ano após o lançamento do primeiro satélite artificial da história, o Sputnik 1, pela URSS, os EUA criaram a DARPA (Defense Advanced Research Projects Agency, ou Agência de Projetos de Pesquisa Avançada de Defesa, em português).

A DARPA é fundamental na história da Internet, uma vez que foi responsável pela pesquisa e desenvolvimento de novas tecnologias para fins defensivos e militares, entre elas, a rede de computadores.

Teoria de comutação de pacotes e rede galáctica

Em 1961, Leonard Kleinrock apresentou sua teoria de comutação de pacotes em sua tese de doutorado no MIT.

Ele alegava que dois servidores poderiam se comunicar para enviar e receber informações transportadas por pacotes por meio de uma rede de nós.

Esses pacotes podiam seguir caminhos diferentes, dependendo da saturação da rede, e ser refeitos na chegada ao destino.

Já em 1962, J. C. R. Licklider, chefe da DARPA e pioneiro da Internet, descreveu o conceito de uma rede galáctica para acessar rapidamente dados de qualquer lugar do mundo.

De forma independente, Paul Baran trabalhou na comutação de pacotes na RAND Corporation. Em 1962, ele apresentou um sistema de comunicações que, por meio de computadores conectados a uma rede descentralizada, era imune a ataques externos, já que, se um ou mais nós fossem destruídos, os outros poderiam continuar funcionando.

O objetivo havia sido cumprido! Se essa tecnologia fosse desenvolvida em larga escala, as informações dos EUA estariam protegidas, pois poderiam ser consultadas em qualquer computador.

Rede de longa distância (WAN)

O grande avanço na história da Internet ocorreu em 1965, quando Lawrence G. Roberts, em Massachusetts, e Thomas Merrill, na Califórnia, conectaram um computador TX2 a um Q-32 por uma linha telefônica comutada de baixa velocidade.

O experimento foi um sucesso e é marcado como o acontecimento que criou a primeira WAN (Wide Area Network) da história.

ARPANET

A história da Internet continuou em 1966, quando Roberts entrou na DARPA e criou o plano da ARPANET para desenvolver a primeira rede de comutação de pacotes junto a Robert Kahn e Howard Frank.

Embora o primeiro protótipo de uma rede comutada por pacotes descentralizada já tivesse sido projetado pelo Laboratório Nacional de Física (NPL) do Reino Unido em 1968, ganharia visibilidade somente em 1969, quando um computador da Universidade da Califórnia (UCLA) se conectou com sucesso a outro do Stanford Research Institute (SRI).

A conexão por nós foi tão bem-sucedida que, meses depois, quatro universidades americanas já estavam interconectadas. Assim nasceu a ARPANET!

Nascimento do NCP e do e-mail

Em 1970, a ARPANET estava consolidada com centenas de computadores conectados.

S. Crocker e sua equipe do Network Working Group estabeleceram o protocolo de controle chamado Network Control Protocol (NCP), que permitia o desenvolvimento de aplicativos a partir dos computadores conectados à ARPANET.

Foi assim que, em 1972, Ray Tomlinson criou o software básico de [e-mail](#), que se tornou o aplicativo mais importante da década e mudou a natureza da comunicação e colaboração entre as pessoas.

Seu impacto foi tão grande que a ARPANET se afastou gradativamente do uso militar, aproximando-se do uso científico na disseminação de informações. Por esse motivo, em 1974, mais de 50 universidades americanas estavam conectadas à ARPANET.

Transição da ARPANET para o TCP/IP

Apesar de seu sucesso, o protocolo NCP não era suficiente para se comunicar com redes ou máquinas fora da ARPANET, como redes de pacotes por rádio ou satélite.

Por isso, em 1974 Robert Kahn e Vinton Cerf desenvolveram uma nova versão do protocolo que respondia a um ambiente de rede de arquitetura aberta. Esse novo protocolo foi chamado de TCP/IP.

O protocolo TCP/IP, mais do que agir como um controlador, facilitava a comunicação entre redes sem a necessidade de que estas fizessem alterações em sua interface. Além disso, garanti que nenhum pacote de informações fosse perdido e verificava se eles chegavam na ordem em que haviam sido enviados.

No início dos anos 80, mais precisamente em 1983, a ARPANET mudou o protocolo NCP para o novo TCP/IP. O IP havia se tornado o serviço portador da Infraestrutura de Informação Global.

Em 1985, a Internet já estava consolidada como a principal rede de comunicação com alcance global.

Nascimento da World Wide Web

Mas o avanço não parou por aí. Em 1989, Tim Berners-Lee desenvolveu a World Wide Web para facilitar o trabalho colaborativo no CERN.

Basicamente, a WWW funciona como um sistema de distribuição de documentos de hipertexto ([HTTP](#)) interconectados e acessíveis por meio de um navegador web conectado à Internet.

O sistema se tornou tão popular no CERN que, em 1991, foi aberto ao público externo. Isso foi possível graças à criação do navegador Mosaic em 1993. De fato, sua recepção foi tão rápida que em 1997 havia mais de 200 mil sites.

Comércio na Internet

Você percebeu que as primeiras redes de computadores estavam restritas a um público de cientistas, engenheiros e funcionários do governo? Bem, essa situação não duraria por muito mais tempo.

Com o advento do TCP/IP, redes individuais, educacionais e comerciais começaram a ter acesso à comunicação quase imediata e às informações disponíveis oferecidas pela Internet. A conectividade deixou de ser exclusiva e se tornou disponível para todos graças à WWW.

Assim, a Internet passou a fazer parte de todos os âmbitos da sociedade, incluindo as atividades comerciais, uma vez que consegue satisfazer necessidades e encontrar formas mais adequadas de executar processos, por exemplo, por meio de plataformas digitais.

De fato, o comércio na Internet levou ao desenvolvimento de serviços de rede privada com TCP/IP, o que causou, entre outras coisas, o surgimento da [educação virtual](#) e do [comércio eletrônico](#), a transição do Marketing tradicional para o [Marketing Digital](#) e a chegada da transformação digital.

Google

Após a criação da WWW, o lançamento do Google em 1997 foi um novo ponto de virada na história da Internet. A empresa levou essa rede para um amplo público, oferecendo um navegador amigável.

Hoje, o Google funciona como navegador e mecanismo de busca, conta com quase um bilhão de páginas indexadas e oferece fácil acesso às informações graças aos seus [algoritmos](#).

Redes sociais

As [redes sociais](#) também foram, assim como o Google, um grande acontecimento. Embora não tenha sido o primeiro, o Facebook é o caso mais bem-sucedido de aplicação da Internet como meio de comunicação e informação, fornecendo acesso às notícias e permitindo que as pessoas se comuniquem em tempo real.

O YouTube marcou outro antes e depois na história da Internet, mostrando que ela também serve como meio de entretenimento, eventualmente substituindo a mídia tradicional, como televisão ou rádio.

Com a chegada massiva de usuários à Internet, as empresas perceberam o enorme potencial de impactar o seu público por meio desses canais. É por isso que hoje é impossível falar de Internet sem publicidade e técnicas de SEO.

Internet 2.0

A Internet desencadeou a Quarta Revolução Industrial, levando o mundo a se estabelecer na Era da Informação.

Inclusive, a Internet 2.0 já está sendo tratada como uma nova etapa que permite que os usuários deixem de ser apenas espectadores e passem a interagir e colaborar entre si como criadores de [conteúdo](#).

A Internet 2.0 é uma tendência baseada em desenhar sites centrados no usuário e que facilitem o compartilhamento e a troca de informações.

A linha do tempo da história da Internet é formada por evoluções e méritos compartilhados que levaram a humanidade a transformar seu estilo de vida e mudar para sempre seus hábitos e processos.

<https://rockcontent.com/br/blog/historia-da-internet/>



<https://www.infowester.com/hubswitchrouter.php>

O que é modem?

Um **modem** consiste, originalmente, em um dispositivo que converte sinal analógico para digital e vice-versa. O nome reflete com precisão essa característica, pois vem da combinação das palavras em inglês *MODulator* (modulador) e *DEModulator* (demodulador).

Nos primeiros anos da internet como a conhecemos, os acessos eram feitos basicamente por meio da exploração das redes de telefonia fixa. O problema é que essas redes foram desenvolvidas para transmissão de informação (voz) por meio de sinal analógico, não para tráfego de sinal digital (dados).

É aqui que o modem entra em cena. Cabe a esse dispositivo converter o sinal digital para analógico (processo conhecido como modulação), assim como converter sinal analógico em digital (demodulação).

De modo resumido, o processo de demodulação funciona assim: o provedor de internet transmite o sinal por meio da rede de telefonia, o modem o recebe e, na sequência, o converte em digital para transmissão ao computador que está conectado a ele.

Já no processo de modulação, os dados oriundos do computador são convertidos em sinal analógico para que possam ser demodulados no outro extremo da conexão.

Esse tipo de modem foi predominante por alguns anos, durante o tempo em que as chamadas *conexões discadas* eram as mais comuns. Naquela época (a década de 1990 e início dos anos 2000, basicamente), os modems trabalhavam com largura de banda de apenas 56 Kb/s.

Como o passar do tempo, as conexões discadas foram substituídas por tecnologias muito mais rápidas, como [ADSL](#), [redes móveis 3G e 4G](#), fibra óptica, entre outras.

Por conta disso, é comum encontrarmos aparelhos com nomes como modem ADSL, modem 4G, modem de fibra óptica e assim por diante. Hoje, aceita-se como definição de modem qualquer dispositivo que faz a comunicação entre um computador ou uma rede privada (como o Wi-Fi da sua casa) e a internet.

O que se conhece como modem de fibra óptica, por exemplo, na verdade é um dispositivo chamado ONT (Optical Network Terminal — Terminal de Rede Óptica). Esse aparelho converte o sinal óptico em elétrico para permitir a comunicação, mas não funciona como os modems originais.



O que é hub?

De todos os equipamentos abordados aqui, o **hub** é o mais simples. Basicamente, o que ele faz é interconectar os computadores de uma rede local (também chamada de LAN — *Local Area Network*) baseada em cabos (via de regra, no padrão Ethernet).

Quando o hub recebe dados de um computador (ou seja, de um nó), simplesmente retransmite as informações para todos os outros equipamentos que fazem parte da rede.

Nesse momento, nenhum outro computador consegue transmitir dados. Esse procedimento só passa a ser possível quando o hub tiver transmitido os dados anteriores.

Um hub pode ter várias portas, isto é, entradas para conexão dos cabos de rede oriundos de cada computador. Há aparelhos que trazem oito, 16, 24 e 32 portas, por exemplo. A quantidade varia de acordo com o modelo e o fabricante.

Note que, se um ou mais nós forem desconectados por qualquer razão (defeito em um cabo, por exemplo), a rede continuará funcionando, afinal, o hub é que a mantém.

Também é possível "encadear" hubs, ou seja, ligar um hub em outro para aumentar a quantidade de nós que compõem a rede.

O problema é que os hubs são muito limitados para os padrões atuais. Não é possível usá-los para conectar a LAN à internet, por exemplo. Por isso, eles caíram em desuso.

Somente aplicações muito específicas, como ferramentas que analisam o tráfego de uma rede local, ainda encontram utilidade nos hubs.



Um antigo hub [Netgear](#)

O que é switch?

Podemos dizer que o **switch** é uma versão mais sofisticada do hub. Esse tipo de equipamento também interconecta computadores e outros dispositivos em uma rede, mas cria canais de comunicação do tipo "origem e destino" dentro dela.

Isso significa que os dados saem do dispositivo de origem e são encaminhados pelo switch apenas para o dispositivo de destino, sem que essas informações tenham que ser retransmitidas para todos os nós da rede.

Repare que as LANs mantidas por switches têm comunicação mais eficiente, pois, ao contrário dos hubs, esse tipo de equipamento não exige que os demais nós da rede fiquem em "silêncio" enquanto um transmite dados.

Com um switch, você pode ter um ou mais nós enviando dados ao mesmo tempo em sua rede. Só existirá algum tipo de espera ou bloqueio temporário de dados se esses computadores estiverem tentando se comunicar com o mesmo nó.

Como esse modelo de origem e destino otimiza o fluxo da dados, uma rede baseada em switch está menos suscetível a falhas de comunicação. Além disso, esse tipo de equipamento se mostra bastante adequado a redes relativamente grandes.

Você pode encontrar no mercado switches com oito, 16, 24, 48 ou 96 portas, por exemplo.



Um switch da [Cisco](#)

Switch gerenciável e switch não gerenciável

A indústria trabalha, basicamente, com dois tipos de switches: **switch gerenciável** e **switch não gerenciável**. Os modelos não gerenciáveis são mais simples e baratos, portanto, costumam ser indicados para redes pequenas (como a de um escritório simples) ou que não têm grande fluxo de dados.

Isso porque switch não gerenciáveis são do tipo "plugue e use" (*plug and play*), por assim dizer: tudo o que você precisa fazer é conectar a ele os computadores que fazem parte da rede. Você não pode fazer nenhuma configuração específica neles, a não ser ajustar um ou outro parâmetro ligado ao funcionamento da própria rede.

Um switch gerenciável é diferente. Com ele, você pode configurar vários parâmetros para aumentar a segurança da rede, melhorar o fluxo de dados, priorizar determinado tipo de tráfego, entre outros.

Com switches gerenciáveis, pode-se ainda monitorar a rede, inclusive remotamente. Via de regra, o monitoramento é feito por meio do SNMP (*Simple Network Management Protocol*), um protocolo específico para esse fim.

O que é roteador?

Um **roteador** (*router*) é um equipamento que tem a função básica de receber e direcionar pacotes de dados dentro de uma rede ou para outras redes. Esse tipo de dispositivo é mais avançado do que o switch. Além de executar as funções deste, os roteadores têm como diferencial a capacidade de determinar qual a melhor rota para um pacote de dados chegar ao seu destino.

Nesse sentido, pense por um momento que a rede é uma cidade. Cabe então ao roteador indicar as rotas que estão menos congestionadas ou as que são mais curtas para que um veículo possa chegar o quanto antes a determinado ponto.

Por conta dessa característica, roteadores são indicados para interligar redes. Isso pode ser feito nas mais diferentes configurações. Por exemplo: uma empresa que ocupa um prédio de três andares e tem uma rede em cada um deles pode usar um roteador para interligá-las e, ao mesmo tempo, conectá-las à internet.

Roteadores podem ter diferentes quantidades de portas e trabalhar em conjunto com switches ou mesmo hubs. Além disso, um roteador sempre trás recursos complementares, como ferramentas para [firewall](#), [DHCP](#) e [DNS](#).

Roteador Wi-Fi (wireless ou sem fio)

Até agora, falamos de hub, switch e roteador como equipamentos para redes baseadas em cabos. Mas redes sem fio (*wireless*) são cada vez mais comuns. Usamos as chamadas redes Wi-Fi sobretudo para conectar notebooks, desktops, smartphones, tablets, TVs e vários outros dispositivos à internet.

Esse trabalho é feito por um tipo de equipamento conhecido como **roteador Wi-Fi** (*Wi-Fi router*). O que ele faz, basicamente, é criar uma rede local (ou, lembrando, uma LAN) e conectá-la à internet. Aqui, o trabalho de roteamento consiste, basicamente, em direcionar os pacotes de dados recebidos e enviados entre cada nó da rede e a internet.

Um roteador Wi-Fi pode ter ou não portas para conexão via cabo Ethernet (com isso, a rede se torna mista). Além disso, ele pode trabalhar com velocidades de transmissão de dados diferentes e variar em alcance físico (proporcionado pela antena).

Se você tiver um roteador de 150 ou 300 Mb/s (megabits por segundo), ele deve funcionar bem em uma casa que tem poucos dispositivos conectados, por exemplo. Mas, em um escritório relativamente grande ou para aplicações que exigem muita largura de banda (vídeos online em [resolução 4K](#), por exemplo), roteadores Wi-Fi mais potentes são indicados

Modem roteador

Se você tem um roteador Wi-Fi convencional, é necessário conectar a ele o modem da sua conexão à internet (não importa se baseada em fibra óptica, ADSL ou outra tecnologia) para que os dispositivos da rede possam ficar online.

Geralmente, o modem é fornecido pelo provedor de internet. Mas, em muitos casos, a empresa fornece um **modem roteador** (neste caso, Wi-Fi), isto é, um equipamento que une essas duas funções.

Roteador ao lado de um modem ou modem roteador, qual a melhor abordagem? Depende. Se você tem poucos dispositivos conectados à sua rede, um modem roteador costuma ser suficiente.

Mas é preciso que o equipamento seja compatível com o tipo de conexão que você contratou — um modem roteador para ADSL não vai funcionar com acessos via fibra óptica e vice-versa, só para dar um exemplo.

Agora, suponha que você queira aumentar o alcance físico da rede. Nessas circunstâncias, o ideal é usar o modem associado a um roteador (à parte) que possa oferecer grande capacidade de cobertura.

Ao tomar essa decisão, você não precisa pedir ao provedor para providenciar um aparelho que faz somente o papel de modem: geralmente, é possível desativar a função de roteamento do modem roteador. Para isso, verifique o manual do equipamento, acione o suporte do provedor ou consulte um profissional especializado em redes.

Protocolos de rede

Para que seja possível uma comunicação entre computadores é necessário que algumas

O que são protocolos de rede?

Protocolos de rede são os conjuntos de normas que permitem que duas ou mais máquinas conectadas à internet se comuniquem entre si. Funciona como uma linguagem universal, que pode ser interpretada por computadores de qualquer fabricante, por meio de qualquer sistema operacional.

Eles são responsáveis por pegar os dados transmitidos pela rede e dividi-los em pequenos pedaços, que são chamados de pacotes. Cada pacote carrega em si informações de endereçamento de origem e destino. Os protocolos também são responsáveis pela sistematização das fases de estabelecimento, controle, tráfego e encerramento.

Quais são os principais tipos de protocolos de rede?

Para que a comunicação entre computadores seja realizada corretamente, é necessário que ambos os computadores estejam configurados segundo os mesmos parâmetros e obedeçam aos mesmos padrões de comunicação.

A rede é dividida em camadas, cada uma com uma função específica. Os diversos tipos de protocolos de rede variam de acordo com o tipo de serviço utilizado e a camada correspondente. Conheça a seguir as principais camadas e seus tipos de protocolos principais:

- camada de aplicação: WWW, HTTP, SMTP, Telnet, FTP, SSH, NNTP, RDP, IRC, **SNMP**, POP3, IMAP, SIP, DNS, PING;
- camada de transporte: TCP, UDP, RTP, DCCP, SCTP;
- camada de rede: IPv4, **IPv6**, IPsec, ICMP;
- camada de ligação física: Ethernet, Modem, PPP, FDDi.

1. IP

O protocolo IP, do termo em inglês **Internet Protocol** (Protocolo de Internet) faz parte da camada de internet e é um dos protocolos mais importantes da web. Ele permite a elaboração e transporte dos pacotes de dados, porém sem assegurar a sua entrega.

O destinatário da mensagem é determinado por meio dos campos de endereço IP (endereço do computador), máscara de sub rede (determina parte do endereço que se refere à rede) e o campo gateway estreita por padrão (permite saber qual o computador de destino, caso não esteja localizado na rede local).

FORMATO DO DATAGRAMA IP

O datagrama IP é *a unidade básica de dados* no nível IP. Um datagrama está dividido em duas áreas, uma área de cabeçalho e outra de dados.

O cabeçalho contém toda a informação necessária que identificam o conteúdo do datagrama.

Na área de dados está encapsulado o pacote do nível superior, ou seja um pacote TCP ou UDP.

O formato do datagrama IP é o seguinte:

0	4	8	16	19	24	31
VERS	HLEN	SERVICE TYPE	TOTAL LENGTH			
IDENTIFICATION			FLAGS	FRAGMENT OFFSET		
TIME TO LIVE		PROTOCOL	HEADER CHECKSUM			
SOURCE IP ADDRESS						
DESTINATION IP ADDRESS						
IP OPTIONS (IF ANY)					PADDING	
DATA						

CAMPOS IP

VERS: versão do protocolo IP que foi usada para criar o datagrama (4bits)

HLEN: comprimento do cabeçalho, medido em palavras de 32 bits (4 bits)

TOTAL-LENGTH: este campo proporciona o comprimento do datagrama medido em bytes, incluindo cabeçalho e dados.

SERVICE-TYPE: este campo especifica como o datagrama poderia ser manejado e dividido em [cinco subcomandos](#)

IDENTIFICATION, FLAGS e FRAGMENTS: estes três campos controlam a fragmentação e a união dos datagramas. O campo de identificação contém um único inteiro que identifica o datagrama, é um campo muito importante porque quando um gateway fragmenta um

datagrama, ele copia a maioria dos campos do cabeçalho do datagrama em cada fragmento, então a identificação também deve ser copiada, com o propósito de que o destino saiba quais fragmentos pertencem a quais datagramas. Cada fragmento tem o mesmo formato que um datagrama completo.

FRAGMENT OFFSET: especifica o início do datagrama original dos dados que estão sendo transportados no fragmento. É medido em unidades de 8 bytes.

FLAG: controla a fragmentação.

TTL(Time To Live): especifica o tempo em segundos que o datagrama está permitido a permanecer no sistema Internet. Gateways e hosts que processam o datagrama devem decrementar o campo TTL cada vez que um datagrama passa por eles e devem removê-lo quando seu tempo expirar.

PROTOCOL: especifica qual protocolo de alto nível foi usado para criar a mensagem que está sendo transportada na área de dados do datagrama.

HEADER-CHECKSUM: assegura integridade dos valores do cabeçalho.

SOURCE AND DESTINATION IP ADDRESS: especifica o endereço IP de 32 bits do remetente e receptor.

OPTIONS: é um campo opcional. Este campo varia em comprimento dependendo de quais opções estão sendo usadas. Algumas opções são de um byte, e neste caso este campo é chamado de [Option Code](#) , e está dividido em três campos.

<http://penta2.ufrgs.br/Esmilda/camposip.html>

2. TCP/IP

Trata-se do acrônimo de dois protocolos combinados. São eles o TCP (Transmission Control Protocol — Protocolo de Controle de Transmissão) e IP (Internet Protocol — Protocolo de Internet).

Juntos, são os responsáveis pela base de envio e recebimento de dados por toda a internet. Essa pilha de protocolos é dividida em 4 camadas:

- aplicação: usada para enviar e receber dados de outros programas pela internet. Nessa camada estão os protocolos HTTP, FTP e SMTP;
- transporte: responsável por transportar os arquivos dos pacotes recebidos da camada de aplicação. Eles são organizados e transformados em outros menores, que serão enviados à rede;
- rede: os arquivos empacotados na camada de transporte são recebidos e anexados ao IP da máquina que envia e recebe os dados. Em seguida, eles são enviados pela internet;
- interface: é a camada que executa o recebimento ou o envio de arquivos na web.

Read more: http://www.linhadecodigo.com.br/artigo/134/tutorial-de-tcp_ip-parte-1.aspx#ixzz7OHnHsl4C

Para que os computadores de uma rede possam trocar informações é necessário que todos adotem as mesmas regras para o envio e o recebimento de informações. Este conjunto de regras é conhecido como Protocolo de comunicação. Falando de outra maneira podemos afirmar: “Para que os computadores de uma rede possam trocar informações entre si é necessário que todos estejam utilizando o mesmo protocolo”. No protocolo de comunicação estão definidas todas as regras necessárias para que o computador de destino, “entenda” as informações no formato que foram enviadas pelo computador de origem. Dois computadores com protocolos diferentes instalados, não serão capazes de estabelecer uma comunicação e trocar informações.

Antes da popularização da Internet existiam diferentes protocolos sendo utilizados nas redes das empresas. Os mais utilizados eram os seguintes:

- TCP/IP
- NETBEUI
- IPX/SPX
- Apple Talk

Se colocarmos dois computadores ligados em rede, um com um protocolo, por exemplo o TCP/IP e o outro com um protocolo diferente, por exemplo NETBEUI, estes dois computadores não serão capazes de estabelecer comunicação e trocar informações. Por exemplo, o computador com o protocolo NETBEUI instalado, não será capaz de acessar uma pasta ou uma Impressora compartilhada no computador com o protocolo TCP/IP instalado.

À medida que a Internet começou, a cada dia, tornar-se mais popular, com o aumento exponencial do número de usuários, o protocolo TCP/IP passou a tornar-se um padrão de fato, utilizando não só na Internet, como também nas redes internas das empresas, redes estas que começavam a ser conectadas à Internet. Como as redes

internas precisavam conectar-se à Internet, tinham que usar o mesmo protocolo da Internet, ou seja: TCP/IP.

Dos principais Sistemas Operacionais do mercado, o UNIX sempre utilizou o protocolo TCP/IP como padrão. O Windows dá suporte ao protocolo TCP/IP desde as primeiras versões, porém o TCP/IP somente tornou-se o protocolo padrão a partir do Windows 2000. Ser o protocolo padrão significa que o TCP/IP será instalado durante a instalação do Sistema Operacional, a não ser que um protocolo diferente seja selecionado. Até mesmo o Sistema Operacional Novell, que sempre foi baseado no IPX/SPX como protocolo padrão, passou a adotar o TCP/IP como padrão a partir da versão 5.0.

O que temos hoje, na prática, é a utilização do protocolo TCP/IP na esmagadora maioria das redes. Sendo a sua adoção cada vez maior. Como não poderia deixar de ser, o TCP/IP é o protocolo padrão do Windows 2000 e também do Windows XP. Se durante a instalação, o Windows detectar a presença de uma placa de rede, automaticamente será sugerida a instalação do protocolo TCP/IP.

http://www.linhadecodigo.com.br/artigo/134/tutorial-de-tcp_ip-parte-1.aspx

3. HTTP/HTTPS

O protocolo HTTP (Hypertext Transfer Protocol — Protocolo de Transferência de Hipertexto) é usado para navegação em **sites da internet**. Funciona como uma conexão entre o cliente (browser) e o servidor (site ou domínio).

O navegador envia um pedido de acesso a uma página, e o servidor retorna uma resposta de permissão de acesso. Junto com ela são enviados também os arquivos da página que o usuário deseja acessar.

Já o HTTPS (Hyper Text Transfer Secure — Protocolo de Transferência de Hipertexto Seguro) funciona exatamente como o HTTP, porém, existe uma camada de proteção a mais. Isso significa que os sites que utilizam esse protocolo são de acesso seguro.

O protocolo HTTPS é comumente usado por sites com sistemas de pagamentos. Esse tipo de site depende de proteção que garanta a integridade dos dados, informações de conta e cartão de crédito dos usuários. A **segurança** é feita por meio de uma certificação digital, que cria uma criptografia para impedir ameaças e **ataques virtuais**.

4. FTP

Significa Protocolo de Transferência de Arquivos (do inglês File Transfer Protocol). É a forma mais simples para transferir dados entre dois computadores utilizando a rede.

O protocolo FTP funciona com dois tipos de conexão: a do cliente (computador que faz o pedido de conexão) e do servidor (computador que recebe o pedido de conexão e fornece o arquivo ou documento solicitado pelo cliente).

O FTP é útil caso o usuário perca o acesso ao painel de controle do seu site. Assim sendo, essa ferramenta pode ser usada para realizar ajustes página, adicionar ou excluir arquivos, ou ainda solucionar qualquer outra questão no site.

5. SFTP

Simple Transfer Protocol (Protocolo de Transferência Simples de Arquivos) consiste no protocolo FTP acrescido de uma camada de proteção para arquivos transferidos.

Nele, a troca de informações é feita por meio de pacotes com a tecnologia SSH (Secure Shell – Bloqueio de Segurança), que autenticam e protegem a conexão entre cliente e servidor. O usuário define quantos arquivos serão transmitidos simultaneamente e define um sistema de senhas para reforçar a segurança.

6. SSH

SSH (Secure Shell, já citado acima) é um dos protocolos específicos de segurança de troca de arquivos entre cliente e servidor. Funciona a partir de uma chave pública. Ela verifica e autentica se o servidor que o cliente deseja acessar é realmente legítimo.

O usuário define um sistema de proteção para o site sem comprometer o seu desempenho. Ele fortifica a segurança do projeto e garante maior confiança e estabilidade na transferência de arquivos.

7. SSL

O protocolo SSL (Secure Sockets Layer — Camada de Portas de Segurança) permite a comunicação segura entre os lados cliente e servidor de uma aplicação web, por meio de uma confirmação da identidade de um servidor e a verificação do seu nível de confiança.

Ele age como uma subcamada nos protocolos de comunicação na internet (TCP/IP). Funciona com a autenticação das partes envolvidas na troca de informações.

A conexão SSL é sempre iniciada pelo cliente, que solicita conexão com um site seguro. O browser, então, solicita o envio do Certificado Digital e verifica se ele é confiável, válido, e se está relacionado ao site que fez o envio. Após a confirmação das informações, a chave pública é enviada e as mensagens podem ser trocadas.

8. ICMP

Sigla para Internet Control Message Protocol (Protocolo de Mensagens de Controle da Internet). Esse protocolo autoriza a criação de mensagens relativas ao IP, mensagens de erro e pacotes de teste.

Ele permite gerenciar as informações relativas a erros nas máquinas conectadas. O protocolo IP não corrige esses erros, mas os mostra para os protocolos das camadas

vizinhas. Por isso, o protocolo ICMP é usado pelos roteadores para assinalar um erro, chamado de Delivery Problem (Problema de Entrega).

9. SMTP

Protocolo para transferência de e-mail simples (Simple Mail Transfer Protocol) é comumente utilizado para transferir e-mails de um servidor para outro, em conexão ponto a ponto.

As mensagens são capturadas e enviadas ao protocolo SMTP, que as encaminha aos destinatários finais em um processo automatizado e quase instantâneo. O usuário não tem autorização para realizar o download das mensagens no servidor.

10. TELNET

Protocolo de acesso remoto. É um protocolo padrão da Internet que permite obter uma interface de terminais e aplicações pela web. Fornece regras básicas para ligar um cliente a um intérprete de comando.

Ele tem como base uma conexão TCP para enviar dados em formato ASCII codificados em 8 bits, entre os quais se intercalam sequências de controle Telnet. Assim, fornece um sistema orientado para a comunicação bidirecional e fácil de aplicar.

11. POP3

Acrônimo para Post Office Protocol 3 (Protocolo de Correios 3). É um protocolo utilizado para troca de mensagens eletrônicas. Funciona da seguinte forma: um servidor de email recebe e armazena mensagens. O cliente se autentica ao servidor da caixa postal para poder acessar e ler as mensagens.

Assim, as mensagens armazenadas no servidor são transferidas em sequência para o computador do cliente. Quando a conexão é encerrada as mensagens ainda são acessadas no modo offline.

<https://www.opservices.com.br/protocolos-de-rede/>

https://www.macoratti.net/17/04/cshp_cacs1.htm

<https://www.codeproject.com/Articles/5733/A-TCP-IP-Server-written-in-C>