



GUIA PRÁTICO DE REDES • @DICAS.TI

DO ZERO AO INTERMEDIÁRIO

Um manual simples para entender como a internet funciona:
história, IP, IPv4, IPv6, DNS e Ping — explicado para quem nunca viu
isso antes.

Thiago Yuri de Oliveira Cordeiro
Coordenador de Segurança Eletrônica
[instagram.com/dicas.ti](https://www.instagram.com/dicas.ti)

Sumário

Introdução.....	3
Capítulo 1 — Uma Breve História da Internet	4
Capítulo 2 — Como a Internet Funciona	5
Capítulo 3 — O Que é um Endereço IP	6
Capítulo 4 — IPv4	7
Capítulo 5 — IPv6	8
Capítulo 6 — DNS	9
Capítulo 7 — O Que é Ping	10
Considerações Finais.....	11
Glossário Rápido	12

Introdução

Se você já ouviu termos como "IP", "DNS" ou "ping" e sempre fingiu que entendia, este e-book é para você. A ideia aqui não é te transformar em um especialista de redes da noite para o dia, mas te dar uma base sólida e simples — do tipo que qualquer pessoa consegue acompanhar, mesmo sem nenhuma experiência técnica.

Vamos caminhar juntos por sete etapas: primeiro entendemos de onde a internet veio, depois como ela funciona por trás das telas, e então destrinchamos os conceitos que mais geram dúvida no dia a dia — endereço IP, IPv4, IPv6, DNS e o famoso comando ping.



Como aproveitar melhor este guia

Leia os capítulos na ordem. Cada um foi pensado para construir em cima do anterior, então pular etapas pode deixar algumas explicações mais difíceis de entender.

CAPÍTULO 1

Uma Breve História da Internet

De onde veio essa rede que conecta o mundo inteiro

A internet não nasceu como a conhecemos hoje. Ela começou como um projeto militar e acadêmico, nos Estados Unidos, no final da década de 1960, chamado ARPANET. O objetivo era simples: criar uma rede de computadores capaz de continuar funcionando mesmo que parte dela fosse destruída — por exemplo, em caso de guerra.

Em 1969, a ARPANET conectou quatro universidades americanas. Foi o primeiro passo de uma ideia que, décadas depois, mudaria completamente a forma como o mundo se comunica.

Os anos 70 e 80: o nascimento dos protocolos

Nos anos seguintes, pesquisadores desenvolveram as regras que permitiriam diferentes redes conversarem entre si — um conjunto de protocolos chamado TCP/IP, que até hoje é a base de tudo o que fazemos online. Vamos explicar o que isso significa em detalhes no próximo capítulo.

Os anos 90: a internet chega às casas

Foi em 1991 que Tim Berners-Lee criou a World Wide Web (WWW) — o sistema de páginas e links que a maioria das pessoas confunde com a própria "internet". Na prática, a web é apenas um dos serviços que rodam sobre a internet, assim como o e-mail e as mensagens instantâneas também são.

A partir da metade dos anos 90, provedores começaram a oferecer acesso discado para o público em geral, e a internet deixou de ser algo restrito a universidades e governos.

Os anos 2000 em diante: banda larga, mobilidade e nuvem

- Banda larga substitui a internet discada, tornando a conexão mais rápida e estável.
- Smartphones colocam a internet no bolso de bilhões de pessoas.
- Redes sociais, streaming e computação em nuvem mudam a forma como consumimos e armazenamos informação.
- O número de dispositivos conectados cresce tanto que o mundo precisa criar um novo sistema de endereçamento — o IPv6, que vamos ver mais adiante.



Resumindo

A internet é, na essência, uma rede de redes: milhares de redes menores (de empresas, provedores, universidades e governos) conectadas entre si por regras comuns, permitindo que qualquer computador converse com qualquer outro, em qualquer lugar do mundo.

CAPÍTULO 2

Como a Internet Funciona

O caminho que uma informação percorre até chegar até você

Quando você abre um site ou manda uma mensagem, a informação não viaja de uma vez só, como uma carta inteira. Ela é quebrada em pequenos pedaços chamados pacotes. Cada pacote viaja de forma independente, às vezes por caminhos diferentes, e é remontado no destino final.

Por que dividir em pacotes?

- Se um pacote se perde no caminho, só ele precisa ser reenviado — não a informação inteira.
- Vários pacotes de dispositivos diferentes podem compartilhar o mesmo cabo ou link de internet ao mesmo tempo.
- A rede fica mais resistente a falhas, já que cada pacote pode seguir uma rota diferente até o mesmo destino.

Os protocolos: as regras do jogo

Para que essa troca de pacotes funcione entre computadores de fabricantes e sistemas totalmente diferentes, todos precisam seguir as mesmas regras. Esse conjunto de regras é chamado de protocolo. O mais importante deles é o TCP/IP, na verdade um conjunto de dois protocolos que trabalham juntos:

- IP (Internet Protocol): cuida do endereçamento — garante que cada pacote saiba para onde ir, como o endereço escrito em um envelope.
- TCP (Transmission Control Protocol): cuida da entrega — garante que os pacotes cheguem completos, na ordem certa, e reenvia o que se perdeu pelo caminho.

Um exemplo prático

Imagine que você digita um endereço de site no navegador. Por trás dessa ação simples, acontece o seguinte, em frações de segundo:

1. Seu computador descobre o endereço IP daquele site (usando o DNS, que veremos no capítulo 6).
2. Seu computador monta um pedido e o quebra em pacotes.
3. Os pacotes saem do seu roteador, passam pelo seu provedor de internet, atravessam várias redes intermediárias, até chegar ao servidor do site.
4. O servidor responde, também em pacotes, que percorrem o caminho de volta até você.
5. Seu navegador remonta tudo e exibe a página na tela.

 **Curiosidade**

Esse processo, que envolve várias redes, roteadores e servidores diferentes, geralmente acontece em menos de um segundo. É por isso que a internet parece "instantânea", mesmo fazendo uma viagem de milhares de quilômetros em alguns casos.

CAPÍTULO 3

O Que é um Endereço IP

A identidade de cada dispositivo conectado à rede

Todo dispositivo conectado a uma rede — seu celular, seu notebook, a câmera de segurança do seu prédio, a smart TV — precisa de um endereço único para poder ser encontrado. Esse endereço é o IP (Internet Protocol Address).

Pense no IP como o endereço de uma casa: sem ele, as cartas (pacotes de dados) não saberiam para onde ir. Da mesma forma que dois imóveis não podem ter exatamente o mesmo endereço na mesma cidade, dois dispositivos não podem usar o mesmo IP na mesma rede ao mesmo tempo.

IP público x IP privado

- IP público: é o endereço que identifica sua rede (ou seu provedor) para o resto da internet. É único no mundo todo.
- IP privado: é o endereço usado dentro da sua própria rede local (em casa ou na empresa), para os dispositivos se comunicarem entre si. Pode se repetir em redes diferentes, já que não é visível de fora.

É por isso que sua casa pode ter um único IP público (fornecido pelo seu provedor), enquanto o roteador distribui IPs privados para o celular, o notebook e a smart TV — todos usando aquela mesma "porta de saída" para acessar a internet.

IP dinâmico x IP fixo

- Dinâmico: muda de tempos em tempos, geralmente atribuído automaticamente por um servidor (DHCP) sempre que o dispositivo se conecta.
- Fixo (ou estático): não muda, é configurado manualmente. Muito usado em servidores, câmeras e equipamentos que precisam ser sempre encontrados no mesmo endereço.



Onde isso aparece no dia a dia

Ao configurar uma câmera de segurança ou um roteador MikroTik, é comum definir um IP fixo justamente para garantir que o equipamento sempre esteja no mesmo "endereço" dentro da rede, facilitando o acesso e o monitoramento.

CAPÍTULO 4

IPv4

O sistema de endereçamento mais usado — e por que ele está ficando pequeno

O IPv4 (Internet Protocol versão 4) é o sistema de endereçamento criado nos anos 80 e ainda é o mais utilizado no mundo. Um endereço IPv4 é formado por quatro números, de 0 a 255, separados por pontos. Por exemplo:

192.168.0.1

Cada um desses quatro blocos é chamado de octeto (porque, no fundo, representa 8 bits de informação). No total, o IPv4 permite cerca de 4,3 bilhões de endereços diferentes — um número que parecia gigantesco nos anos 80, mas que hoje é insuficiente diante de bilhões de celulares, computadores, câmeras e outros dispositivos conectados.

Faixas de IP privado (as mais comuns)

- 10.0.0.0 até 10.255.255.255
- 172.16.0.0 até 172.31.255.255
- 192.168.0.0 até 192.168.255.255

Essas faixas foram reservadas para uso interno em redes locais, exatamente para não conflitarem com IPs públicos usados na internet.

O que é máscara de sub-rede

A máscara de sub-rede trabalha junto com o IP para definir duas coisas: qual parte do endereço identifica a rede, e qual parte identifica o dispositivo dentro dela. Uma máscara comum é 255.255.255.0, escrita também como /24.

Na prática, uma máscara /24 permite até 254 dispositivos naquela rede — o suficiente para a maioria das casas e pequenos escritórios.

O que é NAT

Como as faixas de IP privado se repetem em milhões de redes ao redor do mundo, é preciso um mecanismo que "traduza" esses IPs privados para o IP público na hora de sair para a internet. Esse mecanismo se chama NAT (Network Address Translation) e é feito pelo roteador.



Analogia simples

Pense no NAT como a portaria de um condomínio: cada apartamento tem seu próprio "número interno" (IP privado), mas para o mundo de fora, todas as correspondências saem e chegam pelo mesmo endereço do condomínio (o IP público).

CAPÍTULO 5

IPv6

A solução para a falta de endereços na internet

Como vimos, o IPv4 oferece cerca de 4,3 bilhões de endereços. Parece muito, mas com bilhões de smartphones, computadores, geladeiras, câmeras e sensores conectados, esse número já não é suficiente. A solução criada para resolver esse problema é o IPv6.

Por que o IPv6 resolve o problema

Enquanto o IPv4 usa 32 bits (o que gera os tais 4,3 bilhões de combinações), o IPv6 usa 128 bits. Isso não dobra a quantidade de endereços disponíveis — multiplica de uma forma quase incompreensível, o suficiente para dar um IP único a cada grão de areia do planeta, com sobra.

Como é a aparência de um IPv6

Um endereço IPv6 é escrito em oito grupos de números e letras (hexadecimal), separados por dois-pontos. Por exemplo:

2001:0db8:85a3:0000:0000:8a2e:0370:7334

Para facilitar a leitura, é comum omitir grupos de zeros consecutivos, usando "::" uma única vez no endereço. O exemplo acima poderia ser escrito de forma resumida como:

2001:0db8:85a3::8a2e:0370:7334

IPv4 e IPv6 convivem hoje

A transição do IPv4 para o IPv6 é gradual e vem acontecendo há anos. Atualmente, a maioria das redes opera em modo "dual-stack", ou seja, suportando os dois sistemas ao mesmo tempo, até que o IPv6 se torne o padrão predominante.



Não se preocupe em decorar

No dia a dia, você raramente vai precisar digitar um endereço IPv6 manualmente. O importante aqui é entender por que ele existe e qual problema ele resolve.

CAPÍTULO 6

DNS

O "catálogo telefônico" que traduz nomes em endereços

Decorar endereços IP como 172.217.29.14 para acessar cada site seria impraticável. Por isso existe o DNS (Domain Name System): um sistema que traduz nomes fáceis de lembrar, como google.com, para o endereço IP real do servidor correspondente.

Como funciona, passo a passo

1. Você digita um endereço, por exemplo, meusite.com.br, no navegador.
2. Seu dispositivo pergunta a um servidor DNS: "qual é o IP desse nome?"
3. O servidor DNS responde com o endereço IP correspondente.
4. Seu dispositivo usa esse IP para, finalmente, se conectar ao servidor certo.

Tudo isso acontece em milissegundos, geralmente sem você perceber.

Principais tipos de registro DNS

- Registro A: aponta um nome de domínio para um endereço IPv4.
- Registro AAAA: aponta um nome de domínio para um endereço IPv6.
- Registro CNAME: aponta um nome de domínio para outro nome de domínio (um "apelido").
- Registro MX: indica qual servidor é responsável por receber e-mails daquele domínio.

Por que o DNS às vezes "falha"

Quando um site parece "fora do ar" mas na verdade está funcionando normalmente para outras pessoas, muitas vezes o problema está no DNS — seja porque o servidor DNS que você está usando está lento, seja porque uma alteração recente ainda não se espalhou por toda a internet (um processo chamado propagação, que pode levar de minutos a algumas horas).



Dica prática

Trocar o servidor DNS do seu dispositivo (por exemplo, para 8.8.8.8, do Google, ou 1.1.1.1, da Cloudflare) é uma forma simples de tentar resolver problemas de lentidão ou instabilidade ao acessar sites.

CAPÍTULO 7

O Que é Ping

A ferramenta mais simples para saber se uma conexão está viva

Ping é um comando usado para testar se um dispositivo está acessível em uma rede, e quanto tempo a comunicação com ele está levando. É, provavelmente, a primeira ferramenta de diagnóstico que qualquer técnico de redes aprende a usar.

Como funciona

O comando ping envia pequenos pacotes de teste para um endereço IP ou nome de domínio, e espera uma resposta. Se a resposta chegar, você sabe que existe conexão entre os dois pontos. O tempo que a resposta leva para voltar é chamado de latência, medido em milissegundos (ms).

Como usar (Windows, Linux e Mac)

Basta abrir o terminal (Prompt de Comando, no Windows, ou Terminal, no Mac/Linux) e digitar:

ping google.com

O resultado mostra, para cada pacote enviado, se houve resposta e em quanto tempo. Ao final, um resumo indica quantos pacotes foram perdidos e qual foi o tempo médio de resposta.

Como interpretar o resultado

- Resposta rápida (poucos ms): conexão saudável e estável.
- Resposta lenta (muitos ms): pode indicar congestionamento na rede ou distância grande até o servidor.
- "Esgotado o tempo limite do pedido" ou "Destination unreachable": não há resposta — pode ser um problema de conexão, um firewall bloqueando o ping, ou o dispositivo estar desligado.
- Perda de pacotes: quando parte dos pacotes não recebe resposta, o que geralmente indica instabilidade na rede.

Outras ferramentas parecidas

- Tracert (Windows) ou traceroute (Linux/Mac): mostra o caminho completo, "salto a salto", que os pacotes percorrem até o destino — útil para descobrir em qual ponto da rede está um problema.
- Speedtest: mede a velocidade real da sua conexão de internet, em vez de apenas verificar se ela está ativa.



Uso no dia a dia

Sempre que um cliente relatar que "a câmera caiu" ou "o sistema não conecta", o ping costuma ser o primeiro passo: ele já indica rapidamente se o problema está na rede ou em outro lugar.

Considerações Finais

Chegamos ao fim deste guia introdutório. Você agora entende de onde veio a internet, como as informações viajam em forma de pacotes, o que é um endereço IP, a diferença entre IPv4 e IPv6, como o DNS traduz nomes em endereços, e como usar o ping para verificar se uma conexão está funcionando.

Esses são os pilares que sustentam praticamente tudo o que envolve redes — do Wi-Fi de casa até a infraestrutura que mantém câmeras de segurança, sistemas de acesso e alarmes funcionando 24 horas por dia. A partir daqui, os próximos passos naturais são explorar temas como roteadores e switches, firewalls, redes Wi-Fi, VPNs e configuração de equipamentos como o MikroTik.

Networking é uma área que se aprende na prática. Use os comandos e conceitos deste guia no seu dia a dia — mesmo que seja só para entender por que o Wi-Fi de casa está lento — e o resto vem com o tempo.

Glossário Rápido

- Internet: rede mundial que conecta milhares de redes menores entre si.
- Pacote: pequeno pedaço de dados em que uma informação é dividida para viajar pela rede.
- Protocolo: conjunto de regras que permite dispositivos diferentes se comunicarem.
- IP: endereço que identifica um dispositivo em uma rede.
- IPv4: sistema de endereçamento com 32 bits, o mais usado atualmente.
- IPv6: sistema de endereçamento com 128 bits, criado para suprir a falta de endereços do IPv4.
- Máscara de sub-rede: define qual parte de um IP identifica a rede e qual identifica o dispositivo.
- NAT: mecanismo que traduz IPs privados para um IP público, e vice-versa.
- DNS: sistema que traduz nomes de domínio em endereços IP.
- Ping: comando usado para testar se um dispositivo está acessível e medir o tempo de resposta.
- Latência: tempo que um pacote leva para ir e voltar entre dois pontos da rede.
- Roteador: equipamento que direciona o tráfego de dados entre redes diferentes.