I

IP Address: IPv4, IPv6, Public, Private, and Dynamic Types

Learn how IPv4 and IPv6 addresses identify network interfaces, how public, private, static, dynamic, and shared addresses differ, and what IPs reveal.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
3 min

CONTENTS

In this guide

01 What is an IP address, with an example?
02 IPv4 vs. IPv6
03 Public and private IP addresses
04 Static vs. dynamic addresses
05 NAT and shared public addresses
06 How an address is assigned
07 What an IP address can reveal
08 How to find your addresses
09 Privacy and security limits

An **IP address** is a numeric identifier used to deliver Internet Protocol traffic to a network interface. Routers examine address prefixes to move packets toward their destination. An address identifies a network attachment at a point in time; it does not reliably identify one person.

Two IP versions are active: IPv4 uses 32-bit addresses such as `192.0.2.53`, while IPv6 uses 128-bit hexadecimal addresses such as `2001:db8::53`.

01 What is an IP address, with an example?

An IP address tells Internet Protocol where a packet comes from and where it should go. For example, `192.0.2.53` is an IPv4 documentation address and `2001:db8::53` is an IPv6 documentation address; they are safe examples and are not ordinary public hosts. A device may have several IP addresses at the same time.

02 IPv4 vs. IPv6

IPv4 has about 4.3 billion possible numeric values, with many reserved for special purposes. Address scarcity led to widespread NAT and sharing. IPv6 provides a vastly larger address space and supports direct addressing without requiring NAT for conservation. Both versions still need firewalls, authentication, and secure configuration.

03 Public and private IP addresses

A globally routable public address can be used across the Internet subject to routing and policy. RFC 1918 private IPv4 addresses are intended for local networks and are not routed publicly. The exact blocks are explained in Private IP Addressing.

Link-local, loopback, documentation, multicast, and carrier-grade NAT ranges have separate purposes. They should not all be labeled “private.”

04 Static vs. dynamic addresses

A static address remains assigned by configuration or provider policy. A dynamic address is leased and may change. Dynamic does not mean every reconnect produces a new address, and static does not mean the address is publicly reachable. Businesses often request static public addresses for allowlists, VPN endpoints, or self-hosted services.

05 NAT and shared public addresses

A home router commonly maps several private devices to one public IPv4 address. An ISP may also use carrier-grade NAT, sharing an address among multiple customers. Server logs may therefore show the same public IP for many people. Ports, timestamps, provider records, and other evidence are needed for accurate attribution.

06 How an address is assigned

Home and office devices often receive configuration through DHCP for IPv4 and router advertisements or DHCPv6 for IPv6. ISPs receive address resources through regional registries and delegate them to customers. A device can have multiple addresses at once across physical, virtual, VPN, IPv4, and IPv6 interfaces.

07 What an IP address can reveal

Public registration and geolocation databases may estimate the provider, organization, country, or city. Accuracy varies, especially for mobile networks, VPNs, corporate gateways, and shared addresses. An IP alone normally does not reveal a home address or person’s name to an ordinary website, but a provider may associate assignments with subscriber records under applicable process.

08 How to find your addresses

Use `ipconfig` on Windows, `ip address` on Linux, or Network settings on macOS to see interface addresses. These often differ from the public address visible to an Internet service because of NAT or a VPN. Check both IPv4 and IPv6 when troubleshooting.

09 Privacy and security limits

A VPN changes which public source address a destination sees, but shifts trust to the VPN provider and does not hide logged-in identity, cookies, or device compromise. Changing an IP does not remove malware. Protect exposed services with firewall rules, patches, authentication, and monitoring rather than relying on address secrecy.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com