I

Internet Service Provider (ISP): How It Works and How to Choose

Learn how an ISP connects your network to the Internet, what speed and latency measurements mean, what providers can observe, and how to compare plans.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

CONTENTS

In this guide

01 What does ISP stand for?
02 Common Internet connection types
03 Download, upload, latency, and jitter
04 Public IP addresses, NAT, and CGNAT
05 DNS and security services
06 What can an ISP observe?
07 How to compare ISP plans
08 Troubleshooting a slow connection
09 ISP security checklist

An **Internet service provider (ISP)** is an organization that connects subscribers to the Internet. Depending on the service, an ISP may also provide public IP addresses, DNS resolvers, routers, email, telephone, hosting, security filtering, and customer support.

Your home or business network connects to the ISP's access network, which exchanges traffic with other networks and content providers. The path to a website therefore includes more than Wi-Fi and the advertised access speed.

01 What does ISP stand for?

ISP stands for **Internet service provider**. The provider supplies the access link and routes traffic between the subscriber and other Internet networks. An ISP is not the same as a Wi-Fi router: the router connects local devices and shares the subscribed connection, while the ISP operates the external access and upstream network.

02 Common Internet connection types

- **Fiber** can provide high and often symmetrical capacity with low latency.
- **Cable** uses shared local infrastructure and may have lower upload speed.
- **DSL** operates over telephone lines and depends strongly on line distance and quality.
- **Fixed wireless** connects a location through a terrestrial radio link.
- **Mobile broadband** uses cellular networks and varies with coverage and congestion.
- **Satellite** reaches remote areas but latency and weather sensitivity depend on the system.

03 Download, upload, latency, and jitter

Download and upload rates describe data capacity, usually in megabits per second. Latency measures round-trip delay; jitter describes variation in delay. Video calls and gaming may suffer from high latency or jitter even when a speed test reports ample bandwidth. Compare results over wired Ethernet and Wi-Fi to separate the ISP link from the local network.

04 Public IP addresses, NAT, and CGNAT

An ISP may assign a dynamic or static public address. Some providers use carrier-grade NAT (CGNAT), sharing public IPv4 addresses among customers. CGNAT can complicate inbound hosting, some games, remote access, and attribution. It is not the same as the RFC 1918 addresses used inside a home network. See private IP addressing for the exact ranges.

05 DNS and security services

Providers usually offer recursive DNS resolvers and may include parental controls or malicious-domain filtering. Subscribers can sometimes choose another approved resolver. DNS filtering is one security layer; it does not scan every file or make a destination trustworthy. Confirm how encrypted DNS, filtering, and opt-out settings work on the chosen service.

06 What can an ISP observe?

An ISP necessarily handles connection metadata and IP traffic. HTTPS encrypts page content and paths but does not hide all destination and timing information. Visibility varies with protocol, DNS choice, VPN use, provider architecture, and law. A VPN shifts part of the trust from the ISP to the VPN provider; it does not make the user anonymous or protect a compromised device.

07 How to compare ISP plans

1. Check availability and expected speed at the exact address.
2. Compare upload as well as download performance.
3. Review total price after introductory periods, equipment, installation, and taxes.
4. Check data allowances, contract terms, cancellation costs, and outage credits.
5. Ask whether the service uses CGNAT and whether a public or static address is available.
6. Review privacy, network-management, and support policies.

08 Troubleshooting a slow connection

Test one wired device directly through the normal router, pause large transfers, and record latency, packet loss, download, and upload at several times. Restart equipment only after recording useful status information. If every device is affected over Ethernet, contact the ISP with timestamps and test results. If only Wi-Fi is slow, investigate interference, distance, channels, and access-point placement.

09 ISP security checklist

Change router administration credentials, install firmware updates, use WPA2 or WPA3, disable remote administration unless required, and review provider-managed router access. Keep endpoint protections and backups even if the ISP offers filtering. Report routing, DNS, privacy, or billing problems through official support rather than phone numbers found in pop-up ads.

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