An **Internet service provider** (**ISP**) is an organization that provides services accessing and using the Internet . Internet service providers may be organized in various forms, such as commercial, community-owned , non-profit , or otherwise privately owned .

The Internet was developed as a network between government research laboratories and participating departments of universities. By the late 1980s, a process was set in place towards public, commercial use of the Internet. The remaining restrictions were removed by 1995, 4 years after the introduction of the World Wide Web

Hosting ISPs

Internet hosting services provide email, web-hosting, or online storage services. Other services include virtual server , cloud services, or physical server operation.

In the simplest case, a single connection is established to an upstream ISP and is used to transmit data to or from areas of the Internet beyond the home network; this mode of interconnection is often cascaded multiple times until reaching a tier 1 carrier . In reality, the situation is often more complex. ISPs with more than one point of presence (PoP) may have separate connections to an upstream ISP at multiple PoPs, or they may be customers of multiple upstream ISPs and may have connections to each one of them at one or more point of presence.
[1]
Transit ISPs provide large amounts of bandwidth for connecting hosting ISPs and access ISPs.

Wireless ISP

A wireless Internet service provider (WISP) is an Internet service provider with a network

based on wireless networking. Technology may include commonplace Wi-Fi wireless mesh networking, or proprietary equipment designed to operate over open 900 MHz, 2.4 GHz, 4.9, 5.2, 5.4, 5.7, and 5.8 GHz bands or licensed frequencies such as 2.5 GHz (EBS/BRS), 3.65 GHz (NN) and in the UHF band (including the MMDS frequency band) and LMDS.

Network hardware, software and specifications, as well as the expertise of network management personnel are important in ensuring that data follows the most efficient route, and upstream connections work reliably. A tradeoff between cost and efficiency is possibl

Law enforcement and intelligence assistance

Internet service providers in many countries are legally required (e.g., via Communications Assistance for Law Enforcement Act (CALEA) in the U.S.) to allow law enforcement agencies to monitor some or all of the information transmitted by the ISP, or even store the browsing history of users to allow government access if needed (e.g. via the Investigatory Powers Act 2016 in the United Kingdom). Furthermore, in some countries ISPs are subject to monitoring by intelligence agencies. In the U.S., a controversial National Security Agency program known as PRISM provides for broad monitoring of Internet users traffic and has raised concerns about potential violation of the privacy protections in the Fourth Amendment to the United States Constitution.
[1]
Modern ISPs integrate a wide array of surveillance and packet sniffing equipment into their networks, which then feeds the data to law-enforcement/intelligence networks (such as DCSNet in the United States, or SORM in Russia) allowing monitoring of Internet traffic in real time.

Wikipedia