How the Internet Works

Volume 1: Core Infrastructure

Generated: September 11, 2025

A Complete Technical Guide

From Physical Infrastructure to Future Technologies

Table of Contents

Understanding What the Internet Actually Is

The internet is fundamentally a "network of networks" - millions of independent networks choosing to interconnect and exchange data using common protocols. No single entity owns or controls the internet; instead, it operates through voluntary adoption of standards and cooperative agreements between network operators. This decentralized architecture is what makes the internet resilient, scalable, and resistant to censorship or control.

At its core, the internet implements packet switching, where data is broken into small chunks (packets) that travel independently across the network and are reassembled at their destination. This is fundamentally different from older circuit-switched networks like traditional telephone systems, where a dedicated connection was established for the duration of communication. Packet switching allows multiple conversations to share the same infrastructure efficiently, making the internet economically viable and massively scalable.

The internet operates on a layered protocol model, primarily TCP/IP (Transmission Control Protocol/Internet Protocol), where each layer handles specific aspects of communication. This layered approach means changes can be made at one layer without affecting others - for instance, upgrading from copper to fiber optic cables doesn't require changes to web browsers or email programs. This separation of concerns has allowed the internet to evolve continuously while maintaining backward compatibility.

The economic model of the internet is based on peering (free traffic exchange between networks of similar size) and transit (smaller networks paying larger ones for connectivity). This creates a natural hierarchy from small local ISPs through regional networks to massive Tier 1 providers that form the internet's backbone. These economic relationships, combined with technical protocols, create the seamless global network we experience.

Physical Infrastructure Layer

The physical infrastructure of the internet is a vast, complex system spanning the entire globe. It includes everything from massive undersea cables connecting continents to the Wi-Fi router in your home. This infrastructure represents trillions of dollars of investment and decades of construction, yet most of it remains invisible to users.

The Global Cable Network

The backbone of the internet consists of fiber optic cables that can carry terabits of data per second using light pulses. These cables form a mesh topology where multiple paths exist between major points, ensuring redundancy - if one cable is damaged, data automatically routes around the problem. The global cable infrastructure is owned by various entities including telecommunications companies, governments, and consortiums of companies who share construction and maintenance costs.

Fiber Optic Technology:

Fiber optic cables work by transmitting data as pulses of light through strands of glass thinner than human hair. The physics of total internal reflection keeps light trapped within the fiber, allowing it to travel tens of kilometers without significant loss. Modern fiber systems use multiple wavelengths of light simultaneously (wavelength division multiplexing), allowing a single fiber to carry dozens or hundreds of separate data channels.

Single-mode fiber uses laser light traveling in a single path with a core diameter of 8-10 micrometers (smaller than a red blood cell). It's used for long-distance transmission (up to 100km without amplification) and can carry 400 Gbps per wavelength, with 80+ wavelengths per fiber for a total capacity of 30+ Tbps per fiber pair.

Multi-mode fiber allows light to travel in multiple paths with a core diameter of 50-62.5 micrometers. It's used for shorter distances (up to 2km) with less expensive equipment but limited distance, common in data centers and campus networks.

DWDM (Dense Wavelength Division Multiplexing) splits light into 80+ channels at different wavelengths, with each wavelength carrying an independent data stream. It's like having 80 different colored lasers in one fiber, with spacing between wavelengths of 0.8 nanometers (100 GHz) or less.

Submarine Cable Systems:

Undersea cables are engineering marvels that carry 99% of intercontinental internet traffic (satellites handle less than 1%). These cables must withstand immense pressure, ship anchors, earthquakes, and marine life while operating for 25+ years. The investment required is enormous - a trans-Pacific cable system costs $300-500 million.

Cable construction involves multiple layers of protection: the center contains 8-16 fiber pairs in a steel tube, surrounded by a copper conductor carrying 10,000 volts DC to power repeaters, steel wire armoring for protection from fishing trawlers, and a polyethylene sheath for waterproofing. The total diameter ranges from 17-21mm in deep sea to 50mm at shore landings.

Repeaters/Amplifiers are required every 60-100km. They use Erbium-doped fiber amplifiers (EDFAs) to boost the optical signal, powered by constant current from shore stations. They're designed for a 25-year lifespan without maintenance and use redundant components since repair requires expensive ships.

Cable landing stations are highly secure facilities where submarine cables reach land. They house power feed equipment for submarine repeaters, optical line terminating equipment, and connections to terrestrial networks.

Maintenance and repair involves cable ships on standby in strategic locations. Typical repair time is 1-2 weeks using ROVs (remotely operated vehicles) in deep water and grappling hooks to retrieve cable from the ocean floor.

Terrestrial Backbone Networks:

Land-based fiber networks follow predictable paths along highways, railways, and utility rights-of-way. These networks are easier to maintain than submarine cables but face their own challenges including construction permits, weather damage, and accidental cuts during construction work.

Dark fiber refers to unused fiber capacity installed for future use. Installing fiber is expensive, but adding extra strands is cheap. This "dark" fiber (no light signals transmitted) can be leased and "lit" when needed. Major routes have hundreds of fiber strands.

Optical amplification is necessary for boosting signals for long-distance transmission. EDFAs are placed every 80-120km on terrestrial routes, with Raman amplification for ultra-long spans and Optical-electrical-optical (OEO) regeneration for signal cleanup.

Network topology determines how backbone networks are structured. Ring topology provides automatic backup paths, mesh topology offers multiple paths between points, and dual-diverse routing provides two completely separate physical paths.

Last Mile Infrastructure

The "last mile" (or "first mile" from the user's perspective) is often the bottleneck in internet connectivity. While backbone networks have massive capacity, getting that capacity to individual homes and businesses is expensive and technically challenging. Different technologies serve different population densities and geographic conditions.

DSL (Digital Subscriber Line):

DSL technology cleverly reuses existing telephone infrastructure by transmitting data at frequencies above those used for voice calls. This allows internet and phone service to work simultaneously on the same copper wire. While slower than newer technologies, DSL's advantage is that phone lines already reach nearly every building in developed countries.

ADSL (Asymmetric DSL) provides different upload/download speeds with downloads of 1-24 Mbps and uploads of 0.5-3 Mbps. It's distance sensitive - speed decreases with distance from the DSLAM, with a maximum range of 5.5km from the telephone exchange. It uses frequency division: 0-4kHz for voice, 25-138kHz for upload, and 138kHz-1.1MHz for download.

VDSL/VDSL2 (Very-high-bit-rate DSL) offers up to 100 Mbps download and 50 Mbps upload, but with a maximum range of only 1.5km (much shorter than ADSL). It uses frequencies up to 30MHz and is often deployed as FTTC (Fiber to the Cabinet) with VDSL for the final connection.

G.fast represents the latest DSL technology, offering up to 1 Gbps over very short distances (<100m) using frequencies up to 106MHz or 212MHz. It requires fiber very close to premises.

Vectoring reduces interference between lines in the same bundle. DSL lines interfere with each other (crosstalk), but vectoring uses signal processing to cancel interference, potentially doubling speeds in ideal conditions.

Cable Internet (DOCSIS):

Cable internet uses the same coaxial cables that deliver cable television, sharing bandwidth among neighbors in a local area. DOCSIS (Data Over Cable Service Interface Specification) is the standard that allows data transmission over cable TV infrastructure. Unlike DSL, cable internet is a shared medium where neighborhood usage affects individual speeds.

DOCSIS 3.0 is the current widespread deployment, using channel bonding to combine multiple 6MHz channels. Typical configurations use 32 downstream × 8 upstream channels with a theoretical maximum of 1 Gbps down and 200 Mbps up, though real-world speeds are typically 100-400 Mbps.

DOCSIS 3.1 is the latest standard, using OFDM (Orthogonal Frequency Division Multiplexing) for better spectral efficiency. It supports up to 10 Gbps downstream and 1-2 Gbps upstream, includes Low Latency DOCSIS (LLD) for gaming and video calls, and is backward compatible with DOCSIS 3.0.

HFC (Hybrid Fiber-Coaxial) architecture uses fiber from the headend to neighborhood nodes, with coaxial cable for the last few hundred meters. Each node serves 100-2000 homes, with node splitting used to reduce congestion.

Signal challenges include ingress noise (external RF interference entering the system), return path noise (cumulative noise from all homes), and amplifier cascade (each amplifier adds noise and distortion).

Fiber to the Home (FTTH/FTTP):

Fiber to the home represents the gold standard for internet connectivity, offering virtually unlimited bandwidth potential. However, installation costs are high, particularly in areas with existing underground utilities or low population density. Various architectures balance cost and performance.

PON (Passive Optical Network) is the most common FTTH technology. It requires no powered equipment between the central office and customer, using optical splitters to divide the signal among users (passive = no power required). A single fiber can serve 32-128 homes at lower cost than active Ethernet.

GPON (Gigabit PON) follows the ITU-T G.984 standard, providing 2.488 Gbps downstream and 1.244 Gbps upstream, split among up to 64 users. It has a 20km maximum reach and uses different wavelengths for up/down (1490nm down, 1310nm up).

XGS-PON represents 10 Gigabit symmetric PON with 10 Gbps in both directions. It can coexist with GPON on the same fiber using different wavelengths, making it future-proof for decades.

Active Ethernet provides dedicated fiber per customer with point-to-point connections (no sharing). It typically offers 1-10 Gbps with 100 Gbps possible, but is more expensive and common in business installations.

Network Hardware Infrastructure

The internet's routing infrastructure consists of millions of devices working together to forward packets toward their destinations. These range from massive core routers handling terabits per second to home routers managing a single family's devices. Each router makes independent forwarding decisions, creating a resilient system with no single point of failure.

Core Routers

Core routers form the backbone of the internet, handling massive amounts of traffic at major interconnection points. These are room-sized systems costing millions of dollars, designed for maximum throughput and reliability. They must process packets in nanoseconds while maintaining routing tables with nearly a million entries.

The architecture of core routers features modular chassis with replaceable components. The route processor manages routing protocols and tables, line cards serve as interface modules for fiber connections, switch fabric interconnects line cards at terabit speeds, and everything is redundant: power, fans, and processors.

Performance specifications are impressive: throughput exceeds 100+ Tbps switching capacity, port density includes hundreds of 100/400 Gbps ports, packet forwarding handles billions of packets per second, and latency is measured in microseconds through the router.

Routing table management involves handling a BGP table with approximately 950,000 routes (and growing), using FIB (Forwarding Information Base) as an optimized lookup table, TCAM (Ternary Content Addressable Memory) for hardware-accelerated lookups, and route aggregation to reduce table size.

Major vendors include Cisco, Juniper, Huawei, and Nokia (Alcatel-Lucent), using custom ASICs for packet processing, proprietary and open operating systems, and SDN (Software-Defined Networking) capabilities.

Internet Exchange Points (IXPs)

IXPs are physical locations where different networks connect to exchange traffic. They're critical to internet performance and economics, allowing networks to exchange traffic locally rather than routing through distant third parties. Major IXPs handle more traffic than entire countries.

Physical infrastructure includes meet-me rooms (secure spaces for network interconnection), cross-connects (physical cables between networks), switching fabric (typically Ethernet switches for peering), and route servers (optional centralized routing).

Major global IXPs include DE-CIX Frankfurt (10+ Tbps peak traffic), AMS-IX Amsterdam (8+ Tbps peak), IX.br São Paulo (largest in Southern Hemisphere), and LINX London (5+ Tbps peak).

Peering types include bilateral peering (direct connection between two networks), multilateral peering (via route server to many networks), private peering (dedicated fiber between networks), and public peering (shared switching infrastructure).

Economics show cost savings and performance benefits: avoiding transit costs for local traffic, reducing latency by keeping traffic local, improving reliability with direct connections, and monthly port fees ranging from $500-10,000 depending on speed.

Data Center Infrastructure

Data centers are the factories of the digital economy, housing the servers that power everything from Google searches to Netflix streams. Modern hyperscale data centers are engineering marvels, consuming as much power as small cities while maintaining 99.999% uptime. The concentration of computing power requires sophisticated cooling, power, and networking infrastructure.

Physical Design and Construction:

Data center design balances numerous competing requirements: power efficiency, cooling capacity, network connectivity, physical security, and disaster resistance. Location selection considers power availability, network connectivity, natural disaster risk, and local regulations. Modern data centers are increasingly built in cold climates or near renewable energy sources.

Building specifications include 100,000-1,000,000+ square feet of space, 10-200+ MW power capacity, raised floors of 2-4 feet for cooling and cables, ceiling heights of 12-20 feet for hot air return, floor loading of 150-350 pounds per square foot, and seismic bracing in earthquake zones.

Security layers include perimeter fencing with intrusion detection, vehicle barriers and inspection points, biometric access controls, mantrap entries (security airlocks), 24/7 security staff and CCTV, and separate cages for different customers.

Power Systems:

Data centers require massive amounts of reliable power. A single hyperscale facility can consume 100+ MW - enough to power 80,000 homes. Power systems must provide uninterrupted service even during grid failures, with redundancy at every level.

Utility power delivery involves multiple feeds from different substations, medium voltage (13.8kV-35kV) service, on-site substations for voltage step-down, and power factor correction equipment.

UPS (Uninterruptible Power Supply) systems provide battery backup for 5-30 minutes runtime at full load, or flywheel systems for 15-30 seconds for generator start. Types include online double-conversion for best protection, with 94-97% efficiency in eco-mode and modular designs for maintenance without downtime.

Backup generators (typically diesel, sometimes natural gas) provide 2-3 MW per generator typically, with N+1, N+2, or 2N redundancy, 24-72 hours of fuel on-site, monthly testing required, and emissions regulations limiting runtime.

Power distribution includes PDUs (Power Distribution Units) in server racks, automatic transfer switches (ATS), remote power panels (RPP), busway systems for flexibility, and monitoring at the circuit level.

Cooling Systems:

Cooling represents 30-50% of data center energy consumption. Modern facilities use sophisticated techniques to minimize cooling costs while maintaining safe operating temperatures. The trend is toward higher operating temperatures and free cooling where climate permits.

CRAC/CRAH (Computer Room Air Conditioning/Handler) systems include CRAC units with direct expansion (DX) cooling using refrigerant, and CRAH units using chilled water from a central plant. Capacity ranges from 30-150 tons per unit with perimeter or in-row placement.

Hot aisle/Cold aisle configuration has servers facing each other across cold aisles, exhausting hot air into hot aisles. Containment systems prevent mixing with temperature differentials of 20-30°F.

Liquid cooling for high-density deployments includes rear-door heat exchangers (water-cooled doors on racks), direct-to-chip cooling (cold plates on CPUs/GPUs), and immersion cooling (servers submerged in dielectric fluid). These can handle 50+ kW per rack versus 10-15kW for air-cooled systems.

Free cooling uses outside air when cool enough through airside economizers (direct outside air) or waterside economizers (cooling towers). It's effective when outside temperature is below 65°F and can eliminate mechanical cooling 50-90% of the year.

Network Architecture within Data Centers:

Data center networks must handle massive east-west traffic (server to server) in addition to north-south traffic (to/from internet). Modern architectures use leaf-spine topologies for predictable performance and easy scaling.

Traditional three-tier architecture (becoming obsolete) includes core (high-speed backbone switches), aggregation (middle layer for policy and services), and access (top-of-rack switches connecting servers). Problems include bottlenecks and complex spanning tree configurations.

Leaf-spine architecture (modern standard) features leaf switches connecting to servers (48-64 ports typical) and spine switches connecting all leaf switches. Every leaf connects to every spine, providing predictable latency (always two hops between servers) and easy scaling (add

spines for bandwidth, leaves for servers).

Speeds and feeds include server connections at 10/25/50/100 Gbps, leaf-spine links at 40/100/400 Gbps, and oversubscription ratios of 3:1 typical (3Gbps server traffic, 1Gbps uplink capacity).

SDN in data centers provides centralized control plane, programmable forwarding, dynamic load balancing, and microsegmentation for security.