FEATURE

7 types of networks and their use cases

Networks differ based on size, connectivity, coverage and design. This guide explores seven common types of networks, including their benefits and use cases.

Deanna Darah, Associate Site Editor

A computer network is an interconnected system of devices, represented as network nodes, that share information, data and resources among each other.

Depending on the network type, devices can be as simple as computers or smartphones that connect into a network. Larger networks use devices like routers and switches to create the underlying network infrastructure.

Not all networks are the same. There are several types of networks, each existing to support the devices, size and location of the system. Networks also have differing levels of access and forms of connectivity.

Below are seven common types of networks, along with their benefits and use cases.

1. Personal area network

A personal area network (PAN) is the smallest and simplest type of network. PANs connect devices within the range of an individual and are no larger than about 10 meters (m). Because PANs operate in such limited areas of space, most are wireless and provide short-range connectivity with infrared technology.

An example of a wireless PAN is when users connect Bluetooth devices, like wireless headsets, to a smartphone or laptop. Although most PANs are wireless, wired PAN options exist, including USB.

PAN benefits

- **Portability.** Most devices that connect in a PAN are small and can be easily transported.
- **Affordability.** The ability to form a connection between two devices in a PAN without additional wiring is generally less expensive compared to a wired network.
- **Reliability.** PANs guarantee stable connectivity between devices, provided that the devices remain within the 10 m range.
- **Security.** PANs don't directly connect to larger networks, but rather to other devices connected to larger networks. The security of a device in a PAN is contingent upon how secure the intermediary device is within the larger overall network.

PAN use cases

PANs are configured so individual users can connect their devices within their personal vicinity. A literal example of this is a body area network, in which a user physically wears connected devices. Small home networks with computers, printers and other wireless devices are also considered PANs.

Looking ahead, PANs could function as a key player in the world of futurology. Some networking experts have predicted that PANs may be able to optimize and enable IoT systems in both offices and homes.

2. Local area network

A local area network (LAN) is a system where computers and other devices connect to each other in one location. While PANs connect devices around an individual, the scope of a LAN can range from a few meters in a home to hundreds of meters in a large company office. The network topology determines how devices in LANs interconnect.

LANs use both wired and wireless connectivity options. Wireless LAN (WLAN) has surpassed traditional wired LAN in terms of popularity, but wired LAN remains the more secure and reliable option. Wired LANs use physical cables, like Ethernet, and switches; WLANs use devices, like wireless routers and access points, to interconnect network devices through radio frequency waves.

Network administrators can implement security protocols and encryption standards to secure wireless networks. Wired LANs are usually more secure because they require a physical cable to

form a connection and are far less susceptible to compromise.

LAN benefits

- **Resource sharing.** Resource sharing is one of the most important reasons for setting up any network. As more devices connect to each other, they can share more files, data and software among each other.
- **Secure data storage.** Network data is stored in a centralized location that all connected devices can access. Devices must receive permission to access the network, preventing unauthorized users from retrieving sensitive information.
- **Fast communication.** Ethernet cables provide fast, reliable data transmission speeds, which increase the rate of communication between devices.
- **Seamless communication.** Any authorized user can communicate with another on the same network.

LAN use cases

LANs support home offices and corporate network environments, among others. Users in personal home offices can connect their devices and transfer data between each device with little error. Employees in company offices can quickly communicate, share and access the same data and services provided by their organization.

The most common WLAN use case is Wi-Fi. A wireless network can use Wi-Fi radio signals to connect multiple devices in a single location. It's important to note, though, that WLAN and Wi-Fi differ. A Wi-Fi network is a WLAN, but not all WLANs use Wi-Fi.

Virtual LANs

A virtual LAN (VLAN) is a type of LAN configuration that virtually groups network components into segments. Network administrators create VLANs to operate segments as individual systems, separate from the rest of the LAN. VLANs prevent network congestion by isolating LAN traffic for each segment, in turn improving network performance and efficiency, simplifying network management and increasing security.

3. Metropolitan area network

A metropolitan area network (MAN) is an interconnection of several LANs throughout a city, town or municipality. Like LANs, a MAN can use various wired or wireless connectivity options, including fiber optics, Ethernet cables, Wi-Fi or cellular.

MAN benefits

- **Municipal coverage.** A MAN can span an entire city or town, stretching network connectivity by dozens of miles.
- **Efficient networking standards.** MAN configurations typically use IEEE 802.11 networking standards to increase bandwidth capacity and frequency levels, which boost network performance.

- **High-speed connectivity.** Fiber optic cables are the most popular form of MAN connectivity because they provide safe and fast connection data rates.

MAN use cases

The main purpose of a MAN is to have the same network available in several locations. In a LAN, the network is accessible in one location. In a MAN, organizations with LANs in the same municipality -- such as different office buildings -- can extend their network connectivity to those different locations.

Government entities may also configure a MAN to provide public network connectivity to users. An example of this is when municipalities offer free, public Wi-Fi to city residents using wireless MAN technology.

4. Campus network

A campus network, sometimes referred to as a *campus area network* or *CAN*, is a network of interconnected, dispersed LANs. Like MANs, campus networks extend coverage to buildings close in proximity. The difference between the two configurations is that campus networks connect LANs within a limited geographical area, while MANs connect LANs within a larger metro area. The geographical range of a campus network varies from 1 kilometer to 5 km, while MANs can extend to 50 km.

Campus benefits

- **Affordability.** Campus networks cover a smaller geographical area than MANs, so infrastructure costs less to maintain.
- **Easy configuration.** Compared to MANs, campus networks are easier to set up and manage because there is less ground to cover and fewer devices to support.
- **Wi-Fi hotspot creation.** Universities and other organizations with campus networks may set up free Wi-Fi hotspots in areas with high volume to enable easy network access.

Campus use cases

Network administrators commonly set up campus networks to create networks large enough to cover a school or university. The term *campus network* might imply that these networks work only for university environments, but businesses also set up campus networks to distribute one standardized network across buildings in a localized area.

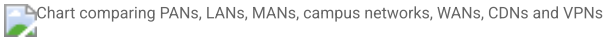
Chart comparing PANs, LANs, MANs, campus networks, WANs, CDNs and VPNs

This table compares the similarities and differences among different network types.

5. Wide area network

A wide area network (WAN) is the most expansive type of computer network configuration. Like a MAN, a WAN is a connection of multiple LANs belonging to the same network. Unlike MANs, however, WANs aren't restricted to the confines of city limits. A WAN can extend to any area of the globe. For example, an organization with a corporate office in New York can connect a branch location in London in the same WAN. Users in both locations obtain access to the same data, files and applications, and can communicate with each other.

WAN benefits

- **Large area coverage.** WANs provide more expansive connectivity because networks can connect from anywhere in the world.
- **Improved performance.** WANs use links with dedicated bandwidth to connect LANs together. These links enhance network speeds and provide faster data transfer rates than LANs.
- **Increased security.** Dedicated links also increase safety across the network because the network only connects to itself, lowering the chances for hackers to hijack a system.

WAN use cases

The main draw of a WAN is its facilitation of long-distance network connectivity. Organizations use WANs to connect branch offices located away from headquarters. But businesses aren't the only ones that can use WANs; an estimated two-thirds of the global population uses the internet -- the world's most popular and largest WAN -- today.

6. Content delivery network

A content delivery network (CDN) is a network of globally distributed servers that deliver dynamic multimedia content -- such as interactive ads or video content -- to web-based internet users. CDNs use specialized servers that deliver bandwidth-heavy rich media content by caching it and speeding up delivery time. CDN providers deploy these digitized servers globally at a network edge, creating geographically distributed points of presence.

When a user requests data in a network, a proxy server forwards the data to the nearest CDN server, which encrypts it into a smaller, more manageable file for the network to handle, before delivering it to the origin server. An origin server provides the content to the user.

CDNs are fairly simple to configure, and organizations have many CDN vendor options from which to purchase services.

CDN benefits

- **Fast content delivery.** The main goal of a CDN is to load rich media content on websites quickly and reduce latency between requests.
- **Increased security.** When traffic travels through a CDN server, potential viruses attached to data reroute to the server, too. A CDN service mitigates these threats so it can send uncompromised data through the network.
- **Improved site performance**. Websites managed by CDNs experience less latency and bandwidth limitation issues. Network downtime caused by traffic spikes is also a rare occurrence in websites with CDNs.

CDN use cases

CDNs enable the delivery of rich -- i.e., dynamic -- media. Most websites and applications incorporate some form of dynamic content, from embedded social media posts to video-streaming players. CDNs are more important than ever for accommodating the vast amount of complex data shared among millions of internet users each day.

7. Virtual private network

A virtual private network (VPN) creates a private network overlay across an existing public network. VPNs use tunneling protocols that create encrypted connections between the network and client devices. Network traffic travels over the VPN service's secure, encrypted tunnels instead of a public network, effectively hiding a user's IP address and data from ISPs and cybersecurity hackers. The user's location appears to be wherever the VPN server exists.

VPN benefits

- **Privacy and anonymity.** Users can browse a network without having their activity monitored by an ISP.
- **Increased security.** Users must receive authentication before gaining access to a VPN. Organizations can secure company data this way by preventing unauthenticated users from accessing sensitive information.

- **Geo-spoofing.** Users connected to VPNs appear to be in the same location as the server, whether in an office building or another country entirely. Users can retrieve company data or gain access to geo-blocked content outside of their country's borders.

VPN use cases

Studies show that VPNs have risen in popularity in recent years as internet users seek to browse the web without surveillance from their ISPs. An ISP can monitor a user's web activity, including sites visited and the types of content downloaded. VPNs hide this information from an ISP, while still providing the user with access to the network service.

VPNs also facilitate remote work for individuals working outside of office locations. User devices with VPN client software can connect to their organization's VPN server and receive access to their office's data center. Using that connection, they can access the same files and resources as employees who are physically located in the building. This functionality made VPN a vital tool during the COVID-19 pandemic, when more than a third of the U.S. labor force worked from home, per Pew Research Center.

Which type of network is the best?

Several network types, associated topologies and methods of connectivity exist -- even beyond this guide. A network professional learning to design a network might wonder which design is the best fit. The simple answer: There isn't one. Choosing which type of network to configure largely depends on the purpose of the system.

Before network professionals decide which type of network to configure, they should first ask a series of questions about the system. Determining the use case of the network, the types of users and devices the network will serve, and the location of the network will help with the process of selecting the network type and connectivity to deploy.

This was last published in April 2022

Dig Deeper on Mobile and wireless network technology

By: Kinza Yasar