Ad-hoc WLAN

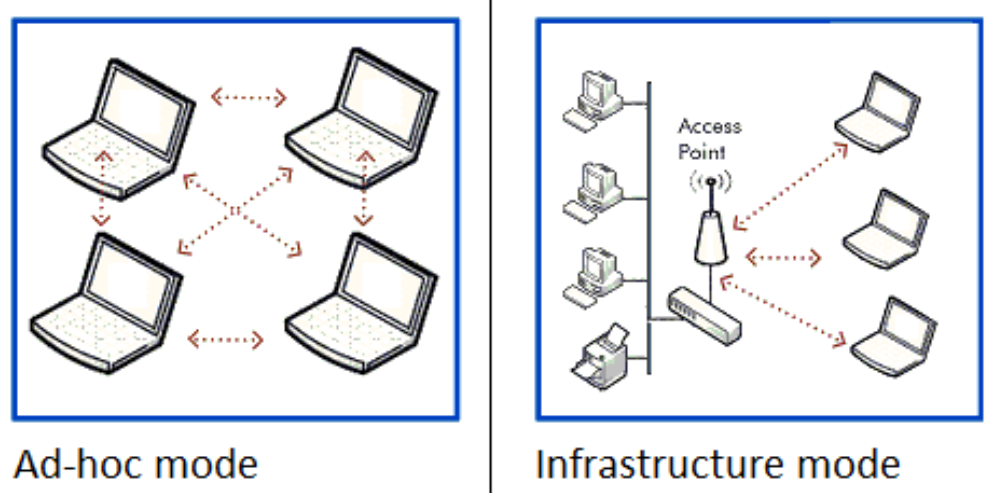
WLANs can be broadly classified into two types, infrastructure networks and ad hoc LANs, based on the underlying architecture.

**Infrastructure networks**

Infrastructure networks contain special nodes called access points (APs), which are connected via existing networks. APs are special in the sense that they can interact with wireless nodes as well as with the existing wired network. The other wireless nodes, also known as mobile stations (STAs), communicate via APs. The APs also act as bridges with other networks.

**Ad hoc networks**

Ad hoc LANs do not need any fixed infrastructure. These networks can be set up on the fly at any place. Nodes communicate directly with each other or forward messages through other nodes that are directly accessible.



**How Ad-hoc network works?**

Because the devices in the ad hoc network can access each other's resources directly through a basic peer-to-peer (P2P) wireless connection, central servers are unnecessary for functions such as file sharing or printing. In a WANET, a collection of devices, or nodes, is responsible for network operations, such as routing, security, addressing and [key management](https://www.techtarget.com/searchdatabackup/definition/encryption-key-management).

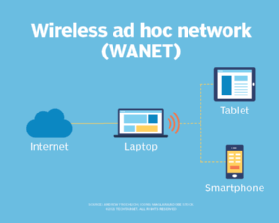
Devices in the ad hoc network require a wireless network adapter or chip, and they need to be able to act as a wireless router when connected. When setting up a wireless ad hoc network, each wireless adapter must be configured for ad hoc mode instead of infrastructure mode. All wireless adapters need to use the same service set identifier ([SSID](https://www.techtarget.com/searchmobilecomputing/definition/service-set-identifier)) and wireless frequency channel number.

Instead of relying on a wireless [base station](https://www.techtarget.com/whatis/definition/base-station) to coordinate the flow of messages to each node in the network, the individual nodes in ad hoc networks forward packets to and from each other. Makeshift by nature, ad hoc wireless networks are useful where there is not a wireless structure built -- for example, if there aren't any access points or routers within range and cabling cannot be extended to reach the location where additional wireless communication is needed.

However, not all Wi-Fi networks are the same. In fact, Wi-Fi access points work in either ad hoc or infrastructure mode. Typically, Wi-Fi networks in infrastructure mode are created and managed using equipment such as Wi-Fi routers, wireless access points ([WAPs](https://www.techtarget.com/searchmobilecomputing/definition/access-point)) and wireless controllers. Ad hoc networks are also often short-lived networks created by a laptop or other device. The use of more sophisticated network protocols and network services found on infrastructure-based wireless networks usually are not suitable for ad hoc networks.

**When should you use an ad hoc wireless network?**

Deciding when to employ ad hoc versus infrastructure mode depends on the use. A user who wants a wireless router to act as a permanent access point should choose infrastructure mode. But ad hoc mode might be a good option for a user setting up a temporary wireless network between a small number of devices.



Connecting devices to the internet using an ad hoc network.

Ad hoc networks are used frequently in new types of wireless engineering. They require minimal configuration and can be deployed quickly, which makes them suitable for emergencies, such as natural disasters or military conflicts. Thanks to the presence of dynamic and [adaptive routing](https://www.techtarget.com/searchnetworking/definition/adaptive-routing) protocols, these networks can be configured quickly. These impromptu, on-demand networks are useful for putting together a small, inexpensive all-wireless LAN without the need for wireless infrastructure equipment. They also work well as a temporary fallback mechanism if equipment for an infrastructure mode network fails.

The following example shows one of the more popular uses for an ad hoc wireless network: connecting multiple wireless endpoints to the internet using an ad hoc intermediary device. Note that the intermediary device consists of a PC or laptop with a wired connection to the internet and a second wireless chip/antenna to connect other ad hoc wireless-capable devices to it for the purpose of sharing internet access.

**Types of ad hoc wireless networks**

Types of WANETs vary by application need and use. Choosing a wireless ad hoc network type depends on the wireless equipment capabilities, physical environment and purpose of the communication.

**MANET.** A mobile ad hoc network involves mobile devices communicating directly with one another. A MANET is a network of wireless mobile devices without an infrastructure that are self-organizing and self-configuring. A MANET is sometimes referred to as an "on-the-fly" or "spontaneous network."

**IMANETs.** Internet-based mobile ad hoc networks support internet protocols, such as TCP/IP (Transmission Control Protocol/Internet Protocol) and User Datagram Protocol ([UDP](https://www.techtarget.com/searchnetworking/definition/UDP-User-Datagram-Protocol)). The iMANET employs a network-layer routing protocol on each connected device to link mobile nodes and set up distributed routes automatically. IMANETs may also be used in the collection of sensor data for data mining for a variety of use cases, such as air pollution monitoring.

**SPANs.** Smartphone ad hoc networks employ existing hardware, such as Wi-Fi and Bluetooth, and software protocols built into a smartphone operating system (OS) to create P2P networks without relying on cellular carrier networks, wireless access points or other traditional network infrastructure equipment. Different from traditional hub-and-spoke networks, such as Wi-Fi Direct, SPANs support multi-hop relays. Multi-hop relay is the process of sending traffic from device A to device C using intermediary device B. Therefore, device A and C do not need to have a direct P2P connection established for traffic to reach its destination. And because SPANs are fully dynamic in nature, there is no notion of a group leader in this type of application and, thus, peers can join or leave without harming the network.

**Vehicular ad hoc network.** This network type involves devices in vehicles that are used for communicating between them and roadside equipment. An example is the in-vehicle safety and security system, OnStar.

### Advantages of a WANET

* Ad hoc mode can be easier to set up than infrastructure mode when just connecting two devices without requiring a centralized access point.
* Because ad hoc networks do not require infrastructure hardware such as access points or wireless routers, these networks provide a low-cost way of direct client-to-client communication.
* Ad hoc networks are easy to configure and offer an effective way to communicate with devices nearby when time is of the essence and running cabling is not feasible.
* Ad hoc networks are often secured to protect against attacks, as their temporary, often impromptu qualities can make them vulnerable to security threats.

### Disadvantages of ad hoc networks

* One major drawback of wireless ad hoc networking is that some Wi-Fi-enabled technology, including certain Android devices, wireless printers and custom IoT sensors, don't support ad hoc mode because of its limitations and will only connect to networks in infrastructure mode by default. In some cases, third-party software can be installed on [endpoint devices](https://www.techtarget.com/searchenterprisedesktop/feature/Endpoint-management-in-a-COVID-19-world) to enable ad hoc communications.
* Infrastructure mode is a better option than ad hoc mode for setting up a larger and more permanent network that can support far more endpoints.
* Ad hoc networks also do not scale well. As the number of devices in an ad hoc network increases, it becomes harder to manage because there is not a central device through which all traffic flows.
* Wireless ad hoc networks cannot bridge wired LANs or to the internet without installing a special-purpose network gateway.
* Devices in an ad hoc network cannot disable SSID broadcasting like devices in infrastructure mode can. As a result, attackers can find and connect to an ad hoc device if they are within signal range.

**Usages of Ad-Hoc network**

* **Military –**  
  An ad hoc networking will give access to the army to maintain an network among all the soldiers, vehicles and headquarters.
* **Personal area network (PAN) –**  
  It is a short range, local network where each nodes are usually related with a given range.
* **Crisis Condition –**  
  Because it is fairly easy to create it can be used in time of crisis to send emergency signals.
* **Medical Application –**  
  It can use to monitor patient.
* **Environmental Application –**  
  It can be used to check weather condition, forest fire, tsunami etc.

**Problems :**  
There are several problems that Ad Hoc network faces –

* Limited wireless range
* Packet losses
* Energy conservation because of limited batteries.
* Low-quality communications.
* Hidden-node problem creates collision if two device try to communicate with same receiver.