**Network Architecture (model)**

**Peer-to-peer architecture**

Often referred to simply as peer-to-peer, or abbreviated P2P, a type of network in which each workstation has equivalent capabilities and responsibilities.

**Client/server architecture**

A network architecture in which each computer or process on the network is either a client or a server.

**P2P**  
often referred to simply as peer-to-peer, or abbreviated P2P, peer-to-peer architecture is a type of network in which each workstation has equivalent capabilities and responsibilities. This differs from client/server architectures where some computers are dedicated to serving the others. Peer-to-peer networks are generally simpler but they usually do not offer the same performance under heavy loads. The P2P network itself relies on computing power at the ends of a connection rather than from within the network itself.

P2P computing takes advantage of existing computing power, computer storage and networking connectivity, allowing users to leverage their collective power to the ‘benefit’ of all.

All nodes are both clients and servers. Each node provides and consumes data and any one node can initiate a connection.

**How Peer-to-peer File-sharing Clients Work**

Once you have downloaded and installed a P2P client, if you are connected to the Internet you can launch the utility and you are then logged into a central indexing server. This central server indexes all users who are currently online connected to the server. This server does not host any files for downloading. The P2P client will contain an area where you can search for a specific file. The utility queries the index server to find other connected users with the file you are looking for. When a match is found the central server will tell you where to find the requested file. You can then choose a result from the search query and your utility when then attempt to establish a connection with the computer hosting the file you have requested. If a successful connection is made, you will begin downloading the file. Once the file download is complete the connection will be broken.

A second model of P2P clients works in the same way but without a central indexing server. In this scenario the P2P software simply seeks out other Internet users using the same program and informs them of your presence online, building a large network of computers as more users install and use the software.

**P2P Security Concerns**

One major concern of using P2P architecture in the workplace is, of course, network security. Security concerns stem from the architecture itself. Today we find most blocking and routing handles by a specific server within network, but the P2P architecture has no single fixed server responsible for routing and requests. The first step in securing your P2P network is to adopt a strict usage policy within the workplace. In securing your network against attacks and viruses there are two main strategies where focus is on controlling the network access or the focus is put on controlling the files. A protocol-based approach is where system administrators use a software or hardware solution to watch for and block intrusive network traffic being received through the P2P clients. A second method of protection is a software solution which would provide file surveillance to actively search for files based on their type, their name, their signature or even their content.

**P2P at Work**

P2P is not only popular with home users but many small businesses have come to rely on this cost-effective solution for sharing files with co-workers and clients. P2P promotes the ease of working together when you're not physically located in the same office. In just seconds updated files and data can be shared with peers and confidential files can be blocked for security. Additionally, companies can also block access to Internet music and video files to assist in maintaining a work-oriented P2P network. Not only does this keep the company free and clear from legal issues regarding music downloading and sharing but it also keeps the corporate bandwidth usage down.

**P2P Characteristics:**

* Clients are also servers and routers: nodes contribute content, storage, memory and CPU.
* Nodes are autonomous (no administrative authority)
* Network is dynamic (nodes enter and leave the network frequently)
* Nodes collaborate directly with each other with having widely varying capabilities

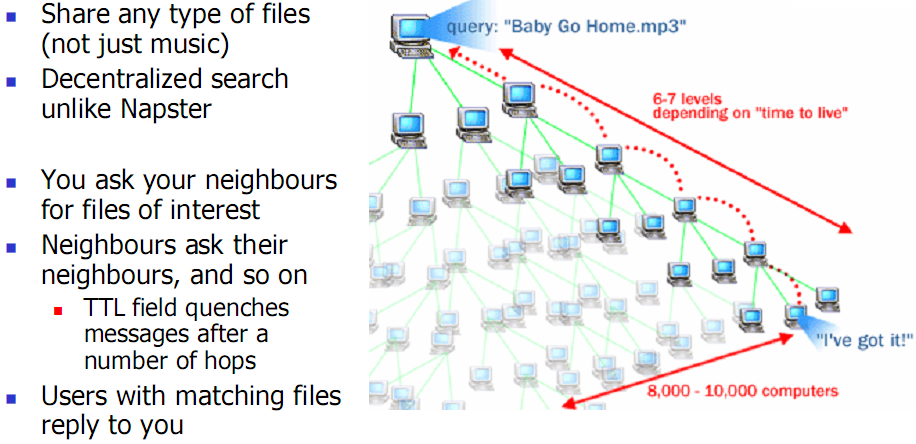
**Benefit:**

* Efficient use of resources: Unused bandwidth, storage, processing power at the edge of the network
* Scalability: consumers of resource also donate resources
* Reliability: no single point of failure
* Ease of administration: built in fault tolerant, replication and load balancing. Nodes self organize.

**Applications:**

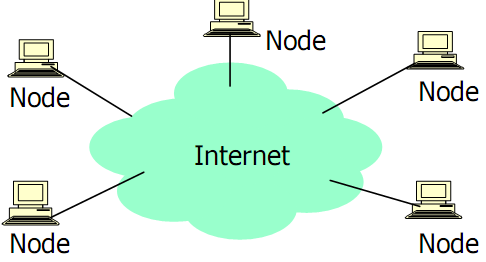
* File sharing (Gnutella, kazaa)
* Multilayer games.
* Collaborative applications
* Distributed computation
* Ad-hoc network.

**Gnutella (example software)**



**Client/Server Architecture**

Client server is a network architecture which separates the client from the server. Each client software can sends request to a server. There are many different types of server like file server, web server, mail server etc..



**Properties:**

|  |  |
| --- | --- |
| Server | Client |
| * Passive (slave) * Waiting for requests * On request serves them and reply | * Active (master) * Sends request * Wait until reply arrives |

Types of client:

**Thin client**: a personal computer that does not have to be very powerful because it only presents the users interface to the user. Largely used for interaction with processing layer.

**Thick client**: a typically powerful personal computer capable of handling independent application processes like notebook computer or PC.

**Types of server**: database server, transaction server (OLTP), OLAP server, Application server, messaging (email, news), web server etc.

**Tired architecture**: Generic client server architecture has two types of nodes on the network: client and server.

**Three tired architecture**: 1. Client tier (web browser).2 application server tier which process data for the clients: a server computer dedicated to running certain software applications (file, print server). 3 database server tier which store data for the application servers: computer program that provide database services to other computer programs. Client tier never communicate with data tier in three tier architecture.

**Wireless LAN**:

A **wireless** [**LAN**](http://en.wikipedia.org/wiki/LAN) or **WLAN** is a [wireless](http://en.wikipedia.org/wiki/Wireless) [local area network](http://en.wikipedia.org/wiki/Local_area_network), which is the linking of two or more computers without using wires. WLAN utilizes [spread-spectrum](http://en.wikipedia.org/wiki/Spread_spectrum) or [OFDM](http://en.wikipedia.org/wiki/OFDM) modulation technology based on [radio waves](http://en.wikipedia.org/wiki/Electromagnetic_radiation) to enable communication between devices in a limited area, also known as the basic service set.

**Architecture:**

All components that can connect into a wireless medium in a [network](http://en.wikipedia.org/wiki/Computer_networking) are referred to as stations. All stations are equipped with wireless [network interface cards](http://en.wikipedia.org/wiki/Network_interface_card) (WNICs). Wireless stations fall into one of two categories: [access points](http://en.wikipedia.org/wiki/Wireless_access_point) and clients.

* **Access points**

Access points (APs) are base stations for the wireless network. They transmit and receive radio frequencies for wireless enabled devices to communicate with.

* **Clients**

Wireless clients can be mobile devices such as laptops, [personal digital assistants](http://en.wikipedia.org/wiki/Personal_digital_assistant), [IP phones](http://en.wikipedia.org/wiki/Voice_over_IP), or fixed devices such as [desktops](http://en.wikipedia.org/wiki/Desktop_computer) and [workstations](http://en.wikipedia.org/wiki/Workstation) that are equipped with a wireless network interface.

**Basic service set**

The basic service set (BSS) is a set of all stations that can communicate with each other. There are two types of BSS: independent BSS and infrastructure BSS. Every BSS has an identification (ID) called the BSSID, which is the [MAC address](http://en.wikipedia.org/wiki/MAC_address) of the access point servicing the BSS.

* **Independent basic service set**

An independent BSS is an [ad-hoc network](http://en.wikipedia.org/wiki/Wireless_ad-hoc_network) that contains no access points, which means they can not connect to any other basic service set.

* **Infrastructure basic service set**

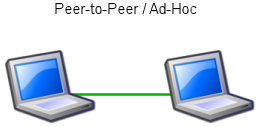
An infrastructure BSS can communicate with other stations not in the same basic service set by communicating through access points.

### Extended service set

An extended service set (ESS) is a set of connected BSSes. Access points in an ESS are connected by a distribution system. Each ESS has an ID called the SSID which is a 32-byte (maximum) character string. For example, "linksys" is the default SSID for Linksys routers.

## Types of wireless LANs

**Peer-to-peer**

[](http://en.wikipedia.org/wiki/Image:Wlan_adhoc.png)

Peer-to-Peer or ad-hoc wireless LAN

A peer-to-peer (P2P) allows wireless devices to directly communicate with each other. Wireless devices within range of each other can discover and communicate directly without involving central access points. This method is typically used by two computers so that they can connect to each other to form a network.

If a signal strength meter is used in this situation, it may not read the strength accurately and can be misleading, because it registers the strength of the strongest signal, which may be the closest computer.

### Bridge

A bridge can be used to connect networks, typically of different types. A wireless Ethernet bridge allows the connection of devices on a wired Ethernet network to a wireless network. The bridge acts as the connection point to the Wireless LAN.

The benefits of wireless LANs include:

* ***Convenience***: The wireless nature of such networks allows users to access network resources from nearly any convenient location within their primary networking environment (home or office). With the increasing saturation of laptop-style computers, this is particularly relevant.
* ***Mobility***: With the emergence of public wireless networks, users can access the internet even outside their normal work environment. Most chain coffee shops, for example, offer their customers a wireless connection to the internet at little or no cost.
* ***Productivity***: Users connected to a wireless network can maintain a nearly constant affiliation with their desired network as they move from place to place. For a business, this implies that an employee can potentially be more productive as his or her work can be accomplished from any convenient location.
* ***Deployment***: Initial setup of an infrastructure-based wireless network requires little more than a single [access point](http://en.wikipedia.org/wiki/Wireless_access_point). Wired networks, on the other hand, have the additional cost and complexity of actual physical cables being run to numerous locations (which can even be impossible for hard-to-reach locations within a building).
* ***Expandability***: Wireless networks can serve a suddenly-increased number of clients with the existing equipment. In a wired network, additional clients would require additional wiring.
* *Cost*: Wireless networking hardware is at worst a modest increase from wired counterparts. This potentially increased cost is almost always more than outweighed by the savings in cost and labor associated to running physical cables

**Disadvantage**:

* ***Security***: Wireless LAN transceivers are designed to serve computers throughout a structure with uninterrupted service using radio frequencies. Because of space and cost, the antennas typically present on wireless networking cards in the end computers are generally relatively poor. In order to properly receive signals using such limited antennas throughout even a modest area, the wireless LAN transceiver utilizes a fairly considerable amount of power. What this means is that not only can the wireless packets be intercepted by a nearby adversary's poorly-equipped computer, but more importantly, a user willing to spend a small amount of money on a good quality antenna can pick up packets at a remarkable distance; perhaps hundreds of times the radius as the typical user. In fact, there are even computer users dedicated to locating and sometimes even cracking into wireless networks, known as [wardrivers](http://en.wikipedia.org/wiki/Wardriving). On a wired network, any adversary would first have to overcome the physical limitation of tapping into the actual wires, but this is not an issue with wireless packets. To combat this consideration, wireless networks users usually choose to utilize various encryption technologies available such as [Wi-Fi Protected Access](http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access) (WPA). Some of the older encryption methods, such as WEP are known to have weaknesses that a dedicated adversary can compromise.
* ***Range***: The typical range of a common [802.11g](http://en.wikipedia.org/wiki/802.11g) network with standard equipment is on the order of tens of meters. While sufficient for a typical home, it will be insufficient in a larger structure. To obtain additional range, [repeaters](http://en.wikipedia.org/wiki/Repeater) or additional access points will have to be purchased. Costs for these items can add up quickly.
* ***Reliability***: Like any radio frequency transmission, wireless networking signals are subject to a wide variety of [interference](http://en.wikipedia.org/wiki/Interference_%28communication%29), as well as complex propagation effects (such as [multipath](http://en.wikipedia.org/wiki/Multipath), or especially in this case [Rician fading](http://en.wikipedia.org/wiki/Rician_fading)) that are beyond the control of the network administrator.
* ***Speed***: The speed on most wireless networks (typically 1-108 Mbit/s) is reasonably slow compared to the slowest common wired networks (100 Mbit/s up to several Gbit/s). There are also performance issues caused by [TCP](http://en.wikipedia.org/wiki/Transmission_Control_Protocol) and its built-in [congestion avoidance](http://en.wikipedia.org/wiki/Network_congestion_avoidance).

Wireless LANs present a host of issues for network managers. Unauthorized access points, broadcasted SSIDs, unknown stations, and spoofed MAC addresses are just a few of the problems addressed in WLAN troubleshooting. Most network analysis vendors, such as Network Instruments, Network General, and Fluke, offer WLAN troubleshooting tools or functionalities as part of their product line.