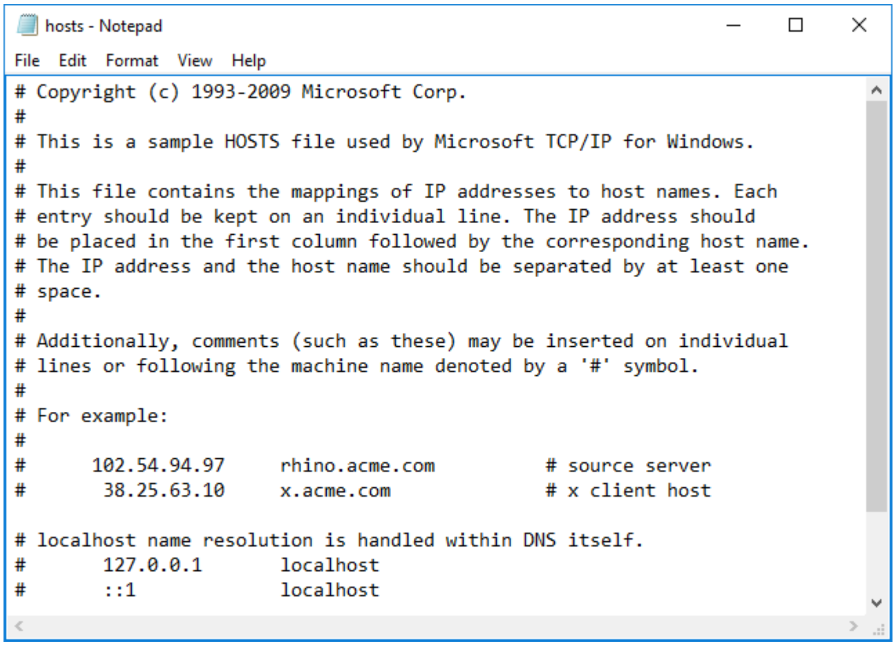
Hosts File

Hosts File

The hosts file on a Windows computer is one method of resolving a host name to an IP address. The file is stored locally on the Windows computer and must be updated manually, which makes this an impractical method for name resolution in a frequently changing network environment. On a Windows 7 or Windows 10 computer, you can locate the hosts file at C:\\Windows\System32\drivers\etc. To view and edit this file, open Notepad as an administrator, and then navigate to the etc directory. The file should look like what is illustrated in Figure 1.



```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
```

Figure 1 Hosts file on Windows 10 computer

As you can see, all name-to-address mappings in the hosts file are commented out with hashmarks (#s), meaning that the computer will ignore any entries in this file. You can allow the computer to read any of the mappings listed in this file by removing the hashmark and saving the file or adding a name-to-address pair without commenting the line entry. Notice that the IPv4 (127.0.0.1) and IPv6 (::1) localhost name-to-address mappings are commented out because Domain Name System (DNS) manages that resolution.

A hosts file can still be used effectively with DNS. For instance, when you add a mapping to the file and save it, the contents of the hosts file are automatically loaded into the DNS client resolver cache, which Windows Sockets applications use for name resolution for both local and remote networks. The primary advantage of using a hosts file is that it is easily edited by the computer's user. The computer user can create easy-to-remember nicknames for hosts and map them to IP addresses in the hosts file. As explained previously, though, this method does not scale well for storing a large number of host names, and maintaining such a file requires a lot of administrative effort.

As you can see in Figure 1, a hosts file can map both IPv4 and IPv6 addresses to computer host names. IPv4 host file entries are unicast addresses using the traditional dotted decimal notation, such as 127.0.0.1, for the localhost. IPv4 entries can also map an IP address to the fully qualified domain name (FQDN), such as the entry 192.168.0.1 srv01.server.home.com s1. The IPv4 address is 192.168.0.1, the FQDN is srv01.server.home.com, and the nickname for the host is s1. Because server name-to-address mappings tend not to change over time, it is probably safe to add this entry, but if the server's address ever changes, then this computer will not be able to resolve the FQDN to the new IP address. It would be ineffective to use a static mapping in a hosts file for a client computer because a computer tends to receive dynamic address assignments from a DHCP server and its IP addresses can change frequently.

IPv6 entries in a hosts file are global or site-local addresses expressed in the traditional colon hexadecimal notation. IPv6 link-local addresses should not be placed in a hosts file because there is no method to specify the zone ID for those addresses. Because link-local addresses are not unique and can be reused on a network, it is possible (however unlikely) that two identical link-local addresses would exist within the same site or organization.

Note: An example of zone ID use is an IPv6 computer with two different network interfaces, each connected to a different subnet. Each interface can have identical IPv6 link-local addresses but use different zone IDs.

The format of a link-local address and zone ID is IPv6_address%zone ID. For example, if the link-local address is fe80::d810:c168:7d19:ee8b%15, the zone ID for this address is 15.

This is the reason you will find only global and site-local IPv6 addresses in a hosts file. Since site-local has been deprecated, you should not add this address type in a local hosts file.

The impetus for DNS came early in the Internet's development. That's because early methods for resolving symbolic names (such as microsoft.com and cengage.com) to numeric IP addresses relied completely on static text files, called HOSTS. The files contained a list of every known host name, their possible aliases, and corresponding numeric IP addresses. This approach was simple to implement and worked on a small scale (under 500 hosts). By 1982, however, the ARPANET (the Internet's government-sponsored predecessor) had around 800 hosts, which made it increasingly difficult to maintain all the HOSTS files needed to translate any and all domain names to their corresponding IP addresses, and vice versa. (See RFC 2235 for a nice Internet timeline.)

When the number of known hosts (and domain names) exceeded 1000 in 1984, maintaining and distributing a current, static HOSTS file for the whole Internet turned into a time-consuming and difficult problem. System administrators began to balk at the requirement to perform daily downloads of increasingly large files, and the environment began growing and changing faster than static methods could handle gracefully.