hosts (file)

The computer file **hosts** is an operating system file that maps hostnames to IP addresses. It is a plain text file. Originally a file named HOSTS.TXT was manually maintained and made available via file sharing by Stanford Research Institute for the ARPANET membership, containing the hostnames and address of hosts as contributed for inclusion by member organizations. The Domain Name System, first described in 1983 and implemented in 1984,[1] automated the publication process and provided instantaneous and dynamic hostname resolution in the rapidly growing network. In modern operating systems, the hosts file remains an alternative name resolution mechanism, configurable often as part of facilities such as the Name Service Switch as either the primary method or as a fallback method.

Contents

Purpose

The hosts file is one of several system facilities that assists in addressing network nodes in a computer network. It is a common part of an operating system's Internet Protocol (IP) implementation, and serves the function of translating human-friendly hostnames into numeric protocol addresses, called IP addresses, that identify and locate a host in an IP network.

In some operating systems, the contents of the hosts file is used preferentially to other name resolution methods, such as the Domain Name System (DNS), but many systems implement name service switches, e.g., nsswitch.conf for Linux and Unix, to provide customization. Unlike remote DNS resolvers, the hosts file is under the direct control of the local computer's administrator.[2]

File content

The hosts file contains lines of text consisting of an IP address in the first text field followed by one or more host names. Each field is separated by white space – tabs are often preferred for historical reasons, but spaces are also used. Comment lines may be included; they are indicated by an octothorpe (#) in the first position of such lines. Entirely blank lines in the file are ignored. For example, a typical hosts file may contain the following:

```
127.0.0.1  localhost loopback
::1        localhost
```

This example only contains entries for the loopback addresses of the system and their host names, a typical default content of the hosts file. The example illustrates that an IP address may have multiple host names (*localhost* and *loopback*), and that a host name may be mapped to both IPv4 and IPv6 IP addresses, as shown on the first and second lines respectively.

Location in the file system

The location of the hosts file in the file system hierarchy varies by operating system. It is usually named *hosts*, without an extension.

Operating System	Version(s)	Location
Unix, Unix-like, POSIX		/etc/hosts[3]
Microsoft Windows	3.1	%WinDir%\HOSTS
	95, 98, ME	%WinDir%\hosts[4]
	NT, 2000, XP,[5] 2003, Vista, 2008, 7, 2012, 8, 10	%SystemRoot%\System32\drivers\etc\hosts[6]
Windows Mobile, Windows Phone		Registry key under HKEY_LOCAL_MACHINE\Comm\Tcpip\Hosts
Apple Macintosh	9 and earlier	Preferences or System folder
	Mac OS X 10.0–10.1.5[7]	(Added through NetInfo or niload)
	Mac OS X 10.2 and newer	/etc/hosts (a symbolic link to */private/etc/hosts*)[7]
Novell NetWare		SYS:etc\hosts
OS/2 & eComStation		"bootdrive":\mptn\etc\
Symbian	Symbian OS 6.1–9.0	C:\system\data\hosts
	Symbian OS 9.1+	C:\private\10000882\hosts
MorphOS	NetStack	ENVARC:sys/net/hosts
AmigaOS	< 4	AmiTCP:db/hosts
	4	DEVS:Internet/hosts
AROS		ENVARC:AROSTCP/db/hosts
Android		/etc/hosts (a symbolic link to */system/etc/hosts*)
iOS	iOS 2.0 and newer	/etc/hosts (a symbolic link to */private/etc/hosts*)
TOPS-20		<SYSTEM>HOSTS.TXT
Plan 9		/lib/ndb/hosts
BeOS		/boot/beos/etc/hosts[8]
Haiku		/boot/common/settings/network/hosts[8]
OpenVMS	UCX	UCX$HOST
	TCPware	TCPIP$HOST
RISC OS	3.7, 5	!Boot.Resources.!Internet.files.Hosts
	later boot sequence	!Boot.Choices.Hardware.Disabled.Internet.Files.Hosts[9]

History

The ARPANET, the predecessor of the Internet, had no distributed host name database. Each network node maintained its own map of the network nodes as needed and assigned them names that were memorable to the users of the system. There was no method for ensuring that all references to a given node in a network were using the same name, nor was there a way to read the hosts file of another computer to automatically obtain a copy.

The small size of the ARPANET kept the administrative overhead small to maintain an accurate hosts file. Network nodes typically had one address and could have many names. As local area TCP/IP computer networks gained popularity, however, the maintenance of hosts files became a larger burden on system administrators as networks and network nodes were being added to the system with increasing frequency.

Standardization efforts, such as the format specification of the file *HOSTS.TXT* in RFC 952, and distribution protocols, e.g., the hostname server described in RFC 953, helped with these problems, but the centralized and monolithic nature of hosts files eventually necessitated the creation of the distributed Domain Name System (DNS).

On some old systems a file named networks is present that has similar to hosts file functions containing names of networks.

Extended applications

In its function of resolving host names, the hosts file may be used to define any hostname or domain name for use in the local system.

Redirecting local domains
: Some web service and intranet developers and administrators define locally defined domains in a LAN for various purposes, such as accessing the company's internal resources or to test local websites in development.

Internet resource blocking
: Entries in the hosts file may be used to block online advertising, or the domains of known malicious resources and servers that contain spyware, adware, and other malware. This may be achieved by adding entries for those sites to redirect requests to another address that does not exist or to a harmless destination. Commercial software applications may be used to populate the hosts file with entries of known undesirable Internet resources automatically.

Security issues

The hosts file may present an attack vector for malicious software. The file may be modified, for example, by adware, computer viruses, or trojan horse software to redirect traffic from the intended destination to sites hosting malicious or unwanted content.[10] The widespread computer worm Mydoom.B blocked users from visiting sites about computer security and antivirus software and also affected access from the compromised computer to the Microsoft Windows Update website.

See also

- DNSBL, a DNS-based blackhole list
- Content-control software
- Ad filtering

References

1. Internet Systems Consortium. "The Most Widely Used Name Server Software: BIND" (http://www.isc.org/downloads/bind/). History of BIND. Retrieved 2017-07-01.
2. "Cisco Networking Academy Program: First-Year Companion Guide", Cisco Systems, Inc., 2002 (2nd Edition), page 676, ISBN 1-58713-025-4
3. "Linux Network Administrators Guide: Writing hosts and networks files" (http://linux.about.com/od/lna_guide/a/gdelna46.htm). Retrieved May 16, 2010.
4. "Hosts File" (http://support.isoc.net/Page.aspx/117/hosts.html). Retrieved August 10, 2011.
5. "Microsoft KB Q314053: TCP/IP and NBT configuration parameters for Windows XP" (https://support.microsoft.com/en-us/kb/314053). Retrieved August 28, 2010.
6. "Microsoft KB 972034 Revision 2.0: default hosts files" (http://support.microsoft.com/kb/972034). Retrieved August 28, 2010.
7. "Mac OS X: How to Add Hosts to Local Hosts File" (http://support.apple.com/kb/TA27291?viewlocale=en_US). Retrieved August 28, 2010.
8. "The Haiku/BeOS Tip Server" (http://betips.net/1997/09/09/aliases-via-the-hosts-file/). Retrieved November 30, 2012.
9. RISC OS 6.14
10. "Remove Trojan.Qhosts – Symantec" (http://www.symantec.com/security_response/writeup.jsp?docid=2003-100116-5901-99&tabid=1). Retrieved May 16, 2010.

External links

- Windows
  - TCP/IP in Windows 2000 Professional (http://www.microsoft.com/technet/prodtechnol/windows2000serv/reskit/prork/prcc_tcp_lesj.mspx?mfr=true)
  - Microsoft TCP/IP Host Name Resolution Order (http://support.microsoft.com/kb/172218)
  - Blocking Unwanted Connections with a Hosts File (Creative Commons License) (http://winhelp2002.mvps.org/hosts.htm)
  - Solution if Windows stops you from modifying the Hosts file or the Lmhosts file in Windows Vista / 7 / 8 (http://support2.microsoft.com/kb/923947)
  - Beginners Guide on Editing Hosts File (http://www.howtogeek.com/howto/27350/beginner-geek-how-to-edit-your-hosts-file/)
  - List of Microsoft related domains that Windows won't redirect (http://www.angelfire.com/comics2/fatboy9175/MShosts.txt)
- Mac
  - How to block unwanted domains with a HOSTS file on Mac OS X 10.2 or later (http://pointhope.de/tips&tricks/no_place_like_localhost.html)
  - "Gas Mask" - Hosts file manager for Mac OS X (http://clockwise.ee)
- Linux
  - Block unwanted advertisements with /etc/hosts file on Linux (http://www.putorius.net/2012/01/block-unwanted-advertisements-on.html)