**Telnet**

From Wikipedia, the free encyclopedia

[Jump to navigation](https://en.wikipedia.org/wiki/Telnet#mw-head) [Jump to search](https://en.wikipedia.org/wiki/Telnet#searchInput)

Not to be confused with [Telenet](https://en.wikipedia.org/wiki/Telenet).

For the Telnet gateway to Wikimedia content, see [meta:Telnet gateway](https://meta.wikimedia.org/wiki/Telnet_gateway)

|  |  |
| --- | --- |
|  | This article **needs additional citations for** [**verification**](https://en.wikipedia.org/wiki/Wikipedia:Verifiability). Please help [improve this article](https://en.wikipedia.org/w/index.php?title=Telnet&action=edit) by [adding citations to reliable sources](https://en.wikipedia.org/wiki/Help:Referencing_for_beginners). Unsourced material may be challenged and removed. *Find sources:* ["Telnet"](https://www.google.com/search?as_eq=wikipedia&q=%22Telnet%22) – [news](https://www.google.com/search?tbm=nws&q=%22Telnet%22+-wikipedia) **·** [newspapers](https://www.google.com/search?&q=%22Telnet%22+site:news.google.com/newspapers&source=newspapers) **·** [books](https://www.google.com/search?tbs=bks:1&q=%22Telnet%22+-wikipedia) **·** [scholar](https://scholar.google.com/scholar?q=%22Telnet%22) **·** [JSTOR](https://www.jstor.org/action/doBasicSearch?Query=%22Telnet%22&acc=on&wc=on) *(April 2014) (*[*Learn how and when to remove this template message*](https://en.wikipedia.org/wiki/Help:Maintenance_template_removal)*)* |

**Telnet** is an [application protocol](https://en.wikipedia.org/wiki/Application_layer) used on the [Internet](https://en.wikipedia.org/wiki/Internet) or [local area network](https://en.wikipedia.org/wiki/Local_Area_Network) to provide a bidirectional interactive text-oriented communication facility using a virtual [terminal](https://en.wikipedia.org/wiki/Text_terminal) connection. User data is interspersed [in-band](https://en.wikipedia.org/wiki/In-band_signaling) with Telnet control information in an 8-bit [byte oriented](https://en.wikipedia.org/wiki/Byte_oriented) data connection over the [Transmission Control Protocol](https://en.wikipedia.org/wiki/Transmission_Control_Protocol) (TCP).

Telnet was developed in 1969 beginning with [RFC 15](https://tools.ietf.org/html/rfc15), extended in [RFC 855](https://tools.ietf.org/html/rfc855), and standardized as [Internet Engineering Task Force](https://en.wikipedia.org/wiki/Internet_Engineering_Task_Force) (IETF) Internet Standard [STD 8](https://en.wikipedia.org/wiki/STD_8), one of the first Internet standards. The name stands for "[**tel**etype](https://en.wikipedia.org/wiki/Teleprinter) **net**work".[[1]](https://en.wikipedia.org/wiki/Telnet#cite_note-1)[[2]](https://en.wikipedia.org/wiki/Telnet#cite_note-2)

Historically, Telnet provided access to a [command-line interface](https://en.wikipedia.org/wiki/Command-line_interface) on a remote host. However, because of serious security concerns when using Telnet over an open network such as the Internet, its use for this purpose has waned significantly in favor of [SSH](https://en.wikipedia.org/wiki/Secure_Shell).

The term *telnet* is also used to refer to the software that implements the client part of the protocol. Telnet client applications are available for virtually all [computer platforms](https://en.wikipedia.org/wiki/Platform_(computing)). *Telnet* is also used as a [verb](https://en.wikipedia.org/wiki/Verb). *To telnet* means to establish a connection using the Telnet protocol, either with a command line client or with a graphical interface. For example, a common directive might be: "*To change your password, telnet into the server, log in and run the* [*passwd*](https://en.wikipedia.org/wiki/Passwd_(command)) *command.*" In most cases, a user would be *telnetting* into a [Unix-like](https://en.wikipedia.org/wiki/Unix-like) server system or a network device (such as a router).

|  |
| --- |
| [**Internet protocol suite**](https://en.wikipedia.org/wiki/Internet_protocol_suite) |
| [**Application layer**](https://en.wikipedia.org/wiki/Application_layer) |
| * [BGP](https://en.wikipedia.org/wiki/Border_Gateway_Protocol) * [DHCP](https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol) * [DNS](https://en.wikipedia.org/wiki/Domain_Name_System) * [FTP](https://en.wikipedia.org/wiki/File_Transfer_Protocol) * [HTTP](https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol) * [HTTPS](https://en.wikipedia.org/wiki/HTTPS) * [IMAP](https://en.wikipedia.org/wiki/Internet_Message_Access_Protocol) * [LDAP](https://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol) * [MGCP](https://en.wikipedia.org/wiki/Media_Gateway_Control_Protocol) * [MQTT](https://en.wikipedia.org/wiki/MQTT) * [NNTP](https://en.wikipedia.org/wiki/Network_News_Transfer_Protocol) * [NTP](https://en.wikipedia.org/wiki/Network_Time_Protocol) * [POP](https://en.wikipedia.org/wiki/Post_Office_Protocol) * [PTP](https://en.wikipedia.org/wiki/Precision_Time_Protocol) * [ONC/RPC](https://en.wikipedia.org/wiki/Open_Network_Computing_Remote_Procedure_Call) * [RTP](https://en.wikipedia.org/wiki/Real-time_Transport_Protocol) * [RTSP](https://en.wikipedia.org/wiki/Real_Time_Streaming_Protocol) * [RIP](https://en.wikipedia.org/wiki/Routing_Information_Protocol) * [SIP](https://en.wikipedia.org/wiki/Session_Initiation_Protocol) * [SMTP](https://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol) * [SNMP](https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol) * [SSH](https://en.wikipedia.org/wiki/Secure_Shell) * Telnet * [TLS/SSL](https://en.wikipedia.org/wiki/Transport_Layer_Security) * [XMPP](https://en.wikipedia.org/wiki/XMPP) * [*more...*](https://en.wikipedia.org/wiki/Category:Application_layer_protocols) |
| [**Transport layer**](https://en.wikipedia.org/wiki/Transport_layer) |
| * [TCP](https://en.wikipedia.org/wiki/Transmission_Control_Protocol) * [UDP](https://en.wikipedia.org/wiki/User_Datagram_Protocol) * [DCCP](https://en.wikipedia.org/wiki/Datagram_Congestion_Control_Protocol) * [SCTP](https://en.wikipedia.org/wiki/Stream_Control_Transmission_Protocol) * [RSVP](https://en.wikipedia.org/wiki/Resource_Reservation_Protocol) * [*more...*](https://en.wikipedia.org/wiki/Category:Transport_layer_protocols) |
| [**Internet layer**](https://en.wikipedia.org/wiki/Internet_layer) |
| * [IP](https://en.wikipedia.org/wiki/Internet_Protocol)   + [IPv4](https://en.wikipedia.org/wiki/IPv4)   + [IPv6](https://en.wikipedia.org/wiki/IPv6) * [ICMP](https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol) * [ICMPv6](https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol_for_IPv6) * [ECN](https://en.wikipedia.org/wiki/Explicit_Congestion_Notification) * [IGMP](https://en.wikipedia.org/wiki/Internet_Group_Management_Protocol) * [IPsec](https://en.wikipedia.org/wiki/IPsec) * [*more...*](https://en.wikipedia.org/wiki/Category:Internet_layer_protocols) |
| [**Link layer**](https://en.wikipedia.org/wiki/Link_layer) |
| * [ARP](https://en.wikipedia.org/wiki/Address_Resolution_Protocol) * [NDP](https://en.wikipedia.org/wiki/Neighbor_Discovery_Protocol) * [OSPF](https://en.wikipedia.org/wiki/Open_Shortest_Path_First) * [Tunnels](https://en.wikipedia.org/wiki/Tunneling_protocol)   + [L2TP](https://en.wikipedia.org/wiki/Layer_2_Tunneling_Protocol) * [PPP](https://en.wikipedia.org/wiki/Point-to-Point_Protocol) * [MAC](https://en.wikipedia.org/wiki/Medium_access_control)   + [Ethernet](https://en.wikipedia.org/wiki/Ethernet)   + [Wi-Fi](https://en.wikipedia.org/wiki/Wi-Fi)   + [DSL](https://en.wikipedia.org/wiki/Digital_subscriber_line)   + [ISDN](https://en.wikipedia.org/wiki/Integrated_Services_Digital_Network)   + [FDDI](https://en.wikipedia.org/wiki/Fiber_Distributed_Data_Interface) * [*more...*](https://en.wikipedia.org/wiki/Category:Link_protocols) |
| * [v](https://en.wikipedia.org/wiki/Template:IPstack) * [t](https://en.wikipedia.org/wiki/Template_talk:IPstack) * [e](https://en.wikipedia.org/w/index.php?title=Template:IPstack&action=edit) |



**Contents**

* [1 History and standards](https://en.wikipedia.org/wiki/Telnet#History_and_standards)
* [2 Security](https://en.wikipedia.org/wiki/Telnet#Security)
* [3 Telnet 5250](https://en.wikipedia.org/wiki/Telnet#Telnet_5250)
* [4 Telnet data](https://en.wikipedia.org/wiki/Telnet#Telnet_data)
* [5 Related RFCs](https://en.wikipedia.org/wiki/Telnet#Related_RFCs)
  + [5.1 Internet Standards](https://en.wikipedia.org/wiki/Telnet#Internet_Standards)
  + [5.2 Proposed Standards](https://en.wikipedia.org/wiki/Telnet#Proposed_Standards)
  + [5.3 Informational/experimental](https://en.wikipedia.org/wiki/Telnet#Informational/experimental)
  + [5.4 Other RFCs](https://en.wikipedia.org/wiki/Telnet#Other_RFCs)
* [6 Telnet clients](https://en.wikipedia.org/wiki/Telnet#Telnet_clients)
* [7 See also](https://en.wikipedia.org/wiki/Telnet#See_also)
* [8 References](https://en.wikipedia.org/wiki/Telnet#References)
* [9 External links](https://en.wikipedia.org/wiki/Telnet#External_links)

**History and standards**

Telnet is a [client-server protocol](https://en.wikipedia.org/wiki/Client-server_protocol), based on a [reliable](https://en.wikipedia.org/wiki/Reliability_(computer_networking)) [connection-oriented](https://en.wikipedia.org/wiki/Connection-oriented) transport. Typically, this protocol is used to establish a connection to [Transmission Control Protocol](https://en.wikipedia.org/wiki/Transmission_Control_Protocol) (TCP) [port number](https://en.wikipedia.org/wiki/Port_number) 23, where a Telnet server application (telnetd) is listening. Telnet, however, predates TCP/IP and was originally run over [Network Control Program](https://en.wikipedia.org/wiki/Network_Control_Program) (NCP) protocols.

Even though Telnet was an ad hoc protocol with no official definition until March 5, 1973,[[3]](https://en.wikipedia.org/wiki/Telnet#cite_note-3) the name actually referred to *Teletype Over Network Protocol* as the [RFC 206](https://tools.ietf.org/html/rfc206) (NIC 7176) on Telnet makes the connection clear:[[4]](https://en.wikipedia.org/wiki/Telnet#cite_note-4)

The TELNET protocol is based upon the notion of a virtual [teletype](https://en.wikipedia.org/wiki/Teleprinter), employing a 7-bit [ASCII](https://en.wikipedia.org/wiki/ASCII) character set. The primary function of a User TELNET, then, is to provide the means by which its users can 'hit' all the keys on that virtual teletype.[[5]](https://en.wikipedia.org/wiki/Telnet#cite_note-5)

Essentially, it used an 8-bit channel to exchange 7-bit ASCII data. Any byte with the high bit set was a special Telnet character. On March 5, 1973, a Telnet protocol standard was defined at [UCLA](https://en.wikipedia.org/wiki/University_of_California,_Los_Angeles)[[6]](https://en.wikipedia.org/wiki/Telnet#cite_note-6) with the publication of two NIC documents: Telnet Protocol Specification, NIC 15372, and Telnet Option Specifications, NIC 15373.

Many extensions were made for Telnet because of its negotiable options protocol architecture. Some of these extensions have been adopted as [Internet standards](https://en.wikipedia.org/wiki/Internet_standard), IETF documents STD 27 through STD 32. Some extensions have been widely implemented and others are proposed standards on the IETF standards track (see [below](https://en.wikipedia.org/wiki/Telnet#Related_RFCs)) Telnet is best understood in the context of a user with a simple terminal using the local Telnet program (known as the client program) to run a logon session on a remote computer where the user's communications needs are handled by a Telnet server program.

**Security**

|  |  |
| --- | --- |
|  | This section **does not** [**cite**](https://en.wikipedia.org/wiki/Wikipedia:Citing_sources) **any** [**sources**](https://en.wikipedia.org/wiki/Wikipedia:Verifiability). Please help [improve this section](https://en.wikipedia.org/w/index.php?title=Telnet&action=edit) by [adding citations to reliable sources](https://en.wikipedia.org/wiki/Help:Referencing_for_beginners). Unsourced material may be challenged and [removed](https://en.wikipedia.org/wiki/Wikipedia:Verifiability#Burden_of_evidence). *(April 2010) (*[*Learn how and when to remove this template message*](https://en.wikipedia.org/wiki/Help:Maintenance_template_removal)*)* |

When Telnet was initially developed in 1969, most users of networked computers were in the computer departments of academic institutions, or at large private and government research facilities. In this environment, security was not nearly as much a concern as it became after the bandwidth explosion of the 1990s. The rise in the number of people with access to the Internet, and by extension the number of people attempting to [hack](https://en.wikipedia.org/wiki/Hacker_(computer_security)) other people's [servers](https://en.wikipedia.org/wiki/Server_(computing)), made encrypted alternatives necessary.

Experts in [computer security](https://en.wikipedia.org/wiki/Computer_security), such as [SANS Institute](https://en.wikipedia.org/wiki/SANS_Institute), recommend that the use of Telnet for remote logins should be discontinued under all normal circumstances, for the following reasons:

* Telnet, by default, does not [encrypt](https://en.wikipedia.org/wiki/Encryption) any data sent over the connection (including passwords), and so it is often feasible to eavesdrop on the communications and use the password later for malicious purposes; anybody who has access to a [router](https://en.wikipedia.org/wiki/Router_(computing)), [switch](https://en.wikipedia.org/wiki/Network_switch), [hub](https://en.wikipedia.org/wiki/Network_hub) or [gateway](https://en.wikipedia.org/wiki/Gateway_(computer_networking)) located on the network between the two hosts where Telnet is being used can intercept the packets passing by and obtain login, password and whatever else is typed with a [packet analyzer](https://en.wikipedia.org/wiki/Packet_analyzer).
* Most implementations of Telnet have no authentication that would ensure communication is carried out between the two desired [hosts](https://en.wikipedia.org/wiki/Server_(computing)) and not [intercepted in the middle](https://en.wikipedia.org/wiki/Man-in-the-middle_attack).
* Several [vulnerabilities](https://en.wikipedia.org/wiki/Vulnerability_(computer_science)) have been discovered over the years in commonly used Telnet [daemons](https://en.wikipedia.org/wiki/Daemon_(computer_software)).

These security-related shortcomings have seen the usage of the Telnet protocol drop rapidly,[[7]](https://en.wikipedia.org/wiki/Telnet#cite_note-7) especially on the public [Internet](https://en.wikipedia.org/wiki/Internet), in favor of the [Secure Shell](https://en.wikipedia.org/wiki/Secure_Shell) (SSH) protocol, first released in 1995. SSH has practically replaced Telnet, and the older protocol is used these days only in rare cases to access decades old legacy equipment that does not support more modern protocols.[[8]](https://en.wikipedia.org/wiki/Telnet#cite_note-8) SSH provides much of the functionality of telnet, with the addition of strong encryption to prevent sensitive data such as passwords from being intercepted, and [public key](https://en.wikipedia.org/wiki/Public_key) authentication, to ensure that the remote computer is actually who it claims to be. As has happened with other early Internet protocols, extensions to the Telnet protocol provide [Transport Layer Security](https://en.wikipedia.org/wiki/Transport_Layer_Security) (TLS) security and [Simple Authentication and Security Layer](https://en.wikipedia.org/wiki/Simple_Authentication_and_Security_Layer) (SASL) authentication that address the above concerns. However, most Telnet implementations do not support these extensions; and there has been relatively little interest in implementing these as SSH is adequate for most purposes.

It is of note that there are a large number of industrial and scientific devices which have only Telnet available as a communication option. Some are built with only a standard RS-232 port and use a serial server hardware appliance to provide the translation between the TCP/Telnet data and the RS-232 serial data. In such cases, SSH is not an option unless the interface appliance can be configured for SSH.

Telnet is still used by hobbyists, especially among [Amateur radio](https://en.wikipedia.org/wiki/Amateur_radio) operators. The [Winlink](https://en.wikipedia.org/wiki/Winlink) protocol supports packet radio via a Telnet connection.

**Telnet 5250**

IBM 5250 or 3270 workstation emulation is supported via custom telnet clients, TN5250/[TN3270](https://en.wikipedia.org/wiki/Telnet_3270), and [IBM servers](https://en.wikipedia.org/wiki/IBM_System_i). Clients and servers designed to pass [IBM 5250](https://en.wikipedia.org/wiki/IBM_5250) data streams over Telnet generally do support [SSL](https://en.wikipedia.org/wiki/Secure_Sockets_Layer) encryption, as SSH does not include 5250 emulation. Under [OS/400](https://en.wikipedia.org/wiki/OS/400) (also known as [IBM i](https://en.wikipedia.org/wiki/IBM_i)), port 992 is the default port for secured telnet.[[9]](https://en.wikipedia.org/wiki/Telnet#cite_note-9)

**Telnet data**

All data [octets](https://en.wikipedia.org/wiki/Octet_(computing)) except 0xff are transmitted over Telnet as is. (0xff, or 255 in decimal, is the IAC byte (Interpret As Command) which signals that the next byte is a telnet command. The command to insert 0xff into the stream is 0xff, so 0xff must be escaped by doubling it when sending data over the telnet protocol.)

Some use Telnet client applications to establish an interactive TCP session to a port other than the Telnet server port. Connections to such ports do not use IAC and all octets are sent to the server without interpretation. For example, a user could make an HTTP request by hand by using a [command line](https://en.wikipedia.org/wiki/Command-line_interface) version of the telnet client to a web server on TCP port 80 as follows:

$ telnet www.example.com 80

GET /path/to/file.html HTTP/1.1

Host: www.example.com

Connection: close

However such services are implemented through *network virtual terminal* (NVT) rules and Telnet does not handle some of the other NVT requirements, such as the requirement for a bare carriage return character (CR, [ASCII](https://en.wikipedia.org/wiki/ASCII) 13) to be followed by a NUL (ASCII 0) character.

There are other TCP terminal clients, such as [netcat](https://en.wikipedia.org/wiki/Netcat) or [socat](https://en.wikipedia.org/wiki/Socat) on UNIX and [PuTTY](https://en.wikipedia.org/wiki/PuTTY) on Windows, which handle such requirements. Nevertheless, Telnet may still be used in [debugging](https://en.wikipedia.org/wiki/Debug) network services such as [SMTP](https://en.wikipedia.org/wiki/SMTP), [IRC](https://en.wikipedia.org/wiki/Internet_Relay_Chat), [HTTP](https://en.wikipedia.org/wiki/HTTP), [FTP](https://en.wikipedia.org/wiki/FTP) or [POP3](https://en.wikipedia.org/wiki/POP3), to issue commands to a server and examine the responses.

Another difference between Telnet and other TCP terminal clients is that Telnet is not [8-bit clean](https://en.wikipedia.org/wiki/8-bit_clean) by default. 8-bit mode may be negotiated, but octets with the high bit set may be garbled until this mode is requested, as 7 bit is the default mode. The 8-bit mode (so named *binary option*) is intended to transmit binary data, not ASCII characters. The standard suggests the interpretation of codes 0000–0176 as ASCII, but does not offer any meaning for high-bit-set *data* octets. There was an attempt to introduce a switchable character encoding support like HTTP has,[[10]](https://en.wikipedia.org/wiki/Telnet#cite_note-10) but nothing is known about its actual software support.

**Related RFCs**

**Internet Standards**

* [RFC 854](https://tools.ietf.org/html/rfc854), Telnet Protocol Specification
* [RFC 855](https://tools.ietf.org/html/rfc855), Telnet Option Specifications
* [RFC 856](https://tools.ietf.org/html/rfc856), Telnet Binary Transmission
* [RFC 857](https://tools.ietf.org/html/rfc857), Telnet Echo Option
* [RFC 858](https://tools.ietf.org/html/rfc858), Telnet Suppress Go Ahead Option
* [RFC 859](https://tools.ietf.org/html/rfc859), Telnet Status Option
* [RFC 860](https://tools.ietf.org/html/rfc860), Telnet Timing Mark Option
* [RFC 861](https://tools.ietf.org/html/rfc861), Telnet Extended Options: List Option

**Proposed Standards**

* [RFC 885](https://tools.ietf.org/html/rfc885), Telnet End of Record Option
* [RFC 1073](https://tools.ietf.org/html/rfc1073), Telnet Window Size Option
* [RFC 1079](https://tools.ietf.org/html/rfc1079), Telnet Terminal Speed Option
* [RFC 1091](https://tools.ietf.org/html/rfc1091), Telnet Terminal-Type Option
* [RFC 1096](https://tools.ietf.org/html/rfc1096), Telnet X Display Location Option
* [RFC 1123](https://tools.ietf.org/html/rfc1123), Requirements for Internet Hosts - Application and Support
* [RFC 1184](https://tools.ietf.org/html/rfc1184), Telnet Linemode Option
* [RFC 1372](https://tools.ietf.org/html/rfc1372), Telnet Remote Flow Control Option
* [RFC 1572](https://tools.ietf.org/html/rfc1572), Telnet Environment Option
* [RFC 2941](https://tools.ietf.org/html/rfc2941), Telnet Authentication Option
* [RFC 2942](https://tools.ietf.org/html/rfc2942), Telnet Authentication: Kerberos Version 5
* [RFC 2943](https://tools.ietf.org/html/rfc2943), TELNET Authentication Using DSA
* [RFC 2944](https://tools.ietf.org/html/rfc2944), Telnet Authentication: SRP
* [RFC 2946](https://tools.ietf.org/html/rfc2946), Telnet Data Encryption Option
* [RFC 4248](https://tools.ietf.org/html/rfc4248), The telnet URI Scheme

**Informational/experimental**

* [RFC 1143](https://tools.ietf.org/html/rfc1143), The Q Method of Implementing TELNET Option Negotiation
* [RFC 1571](https://tools.ietf.org/html/rfc1571), Telnet Environment Option Interoperability Issues

**Other RFCs**

* [RFC 1041](https://tools.ietf.org/html/rfc1041), Telnet 3270 Regime Option
* [RFC 1205](https://tools.ietf.org/html/rfc1205), 5250 Telnet Interface
* [RFC 2217](https://tools.ietf.org/html/rfc2217), Telnet Com Port Control Option
* [RFC 4777](https://tools.ietf.org/html/rfc4777), IBM's iSeries Telnet Enhancements

**Telnet clients**

* [PuTTY](https://en.wikipedia.org/wiki/PuTTY) and plink command line are a free, open-source [SSH](https://en.wikipedia.org/wiki/Secure_Shell), Telnet, [rlogin](https://en.wikipedia.org/wiki/Rlogin), and [raw TCP](https://en.wikipedia.org/wiki/Transmission_Control_Protocol) [client](https://en.wikipedia.org/wiki/Client_(computing)) for [Windows](https://en.wikipedia.org/wiki/Microsoft_Windows), [Linux](https://en.wikipedia.org/wiki/Linux), and [Unix](https://en.wikipedia.org/wiki/Unix).
* [AbsoluteTelnet](https://en.wikipedia.org/wiki/AbsoluteTelnet) is a telnet client for [Windows](https://en.wikipedia.org/wiki/Microsoft_Windows). It also supports [SSH](https://en.wikipedia.org/wiki/Secure_Shell) and [SFTP](https://en.wikipedia.org/wiki/SSH_File_Transfer_Protocol),
* [RUMBA (Terminal Emulator)](https://en.wikipedia.org/wiki/RUMBA_(Terminal_Emulator))
* [Line Mode Browser](https://en.wikipedia.org/wiki/Line_Mode_Browser), a command line [web browser](https://en.wikipedia.org/wiki/Web_browser)
* [NCSA Telnet](https://en.wikipedia.org/wiki/NCSA_Telnet)
* [TeraTerm](https://en.wikipedia.org/wiki/TeraTerm)
* [SecureCRT](https://en.wikipedia.org/wiki/SecureCRT) from Van Dyke Software
* [ZOC Terminal](https://en.wikipedia.org/wiki/ZOC_(software))
* [SyncTERM](https://en.wikipedia.org/wiki/SyncTERM) BBS terminal program supporting Telnet, SSHv2, RLogin, Serial, Windows, \*nix, and Mac OS X platforms, X/Y/ZMODEM and various BBS terminal emulations
* [Rtelnet](https://en.wikipedia.org/wiki/Rtelnet) is a [SOCKS](https://en.wikipedia.org/wiki/SOCKS) client version of Telnet, providing similar functionality of telnet to those hosts which are behind [firewall](https://en.wikipedia.org/wiki/Firewall_(computing)) and [NAT](https://en.wikipedia.org/wiki/Network_address_translation).
* [Inetutils](https://en.wikipedia.org/wiki/Inetutils) includes a telnet client and server and is installed by default on many GNU/Linux distributions.
* telnet.exe command line utility included in default installation of many version of Microsoft Windows OS.

**See also**

* [List of terminal emulators](https://en.wikipedia.org/wiki/List_of_terminal_emulators)
* [Banner grabbing](https://en.wikipedia.org/wiki/Banner_grabbing)
* [Virtual terminal](https://en.wikipedia.org/wiki/Virtual_terminal)
* [Reverse telnet](https://en.wikipedia.org/wiki/Reverse_telnet)
* [HyTelnet](https://en.wikipedia.org/wiki/HyTelnet)
* [Kermit](https://en.wikipedia.org/wiki/Kermit_(protocol))
* [SSH](https://en.wikipedia.org/wiki/Secure_Shell)

**References**

 Andrew Wheen. *Dot-dash to Dot.Com: How Modern Telecommunications Evolved from the Telegraph to the Internet*. Springer, 2011. p. 132. [ISBN](https://en.wikipedia.org/wiki/ISBN_(identifier)) [9781441967596](https://en.wikipedia.org/wiki/Special:BookSources/9781441967596).

  Christoph Meinel; Harald Sack. *Internetworking: Technological Foundations and Applications*. X.media.publishing, 2013. p. 57. [ISBN](https://en.wikipedia.org/wiki/ISBN_(identifier)) [3642353916](https://en.wikipedia.org/wiki/Special:BookSources/3642353916).

  [RFC 318](https://tools.ietf.org/html/rfc318) — documentation of old ad hoc telnet protocol

  Garth O. Bruen. *WHOIS Running the Internet: Protocol, Policy, and Privacy*. Wiley, 1st edition (November 2, 2015). p. 25. [ISBN](https://en.wikipedia.org/wiki/ISBN_(identifier)) [9781118679555](https://en.wikipedia.org/wiki/Special:BookSources/9781118679555).

  [The RFC 206 (NIC 7176)](http://ietf.org/rfc/rfc0206.txt) [Archived](https://web.archive.org/web/20170315080607/http:/ietf.org/rfc/rfc0206.txt) 2017-03-15 at the [Wayback Machine](https://en.wikipedia.org/wiki/Wayback_Machine), 9 August 1971; Computer Research Lab, UCSB; J. White.

  [RFC 495](https://tools.ietf.org/html/rfc495) — announcement of Telnet protocol

  *Poulsen, Kevin (2 April 2007).* [*"Telnet, dead at 35...RIP"*](https://www.wired.com/2007/04/telnet_dead_at_/)*. Wired. April 2007 (2007–04): 24.* [*Archived*](https://web.archive.org/web/20161221012744/https:/www.wired.com/2007/04/telnet_dead_at_/) *from the original on 21 December 2016. Retrieved 14 June 2017.*

  *Ylonen, Tatu.* [*"History of the SSH Protocol"*](https://www.ssh.com/ssh/telnet)*. SSH home page. SSH Communications Security, Inc.* [*Archived*](https://web.archive.org/web/20180725073549/https:/www.ssh.com/ssh/telnet) *from the original on 25 July 2018. Retrieved 14 June 2017.*

  [*"IBM TCP/IP Ports Required for Access for Windows and Related Functions - United States"*](http://www-01.ibm.com/support/docview.wss?uid=nas8N1019667)*. www-01.ibm.com. IBM Technote.* [*Archived*](https://web.archive.org/web/20160918095706/http:/www-01.ibm.com/support/docview.wss?uid=nas8N1019667) *from the original on 2016-09-18. Retrieved 2016-09-07.*

* 1.  [RFC 2066](https://tools.ietf.org/html/rfc2066) — TELNET CHARSET Option

57.9654

**External links**

* [Telnet Options](http://www.iana.org/assignments/telnet-options) — the official list of assigned option numbers at iana.org
* [Telnet Interactions Described as a Sequence Diagram](http://www.eventhelix.com/RealtimeMantra/Networking/Telnet.pdf)
* [Telnet configuration](https://web.archive.org/web/20180702181236/http:/telecomacadmey.com/configure-telnet/)
* [Telnet protocol description, with NVT reference](http://www.pcmicro.com/netfoss/telnet.html)
* [Microsoft TechNet:Telnet commands](https://technet.microsoft.com/en-us/library/bb491013.aspx)
* [TELNET: The Mother of All (Application) Protocols](http://www2.sims.berkeley.edu/courses/is250/s99/articles/w3088.pdf)
* [Troubleshoot Telnet Errors in Windows Operating System](http://www.technig.com/troubleshoot-telnet-errors/)
* [*"telnet.org - information about telnet"*](http://telnet.org/)*. telnet.org. Retrieved 2020-01-07.* Contains a list of telnet addresses and list of telnet clients