Telnet

Not to be confused with Telenet.

Telnet is a session layer protocol used on the Internet or local area networks to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection. User data is interspersed in-band with Telnet control information in an 8-bit byte oriented data connection over the Transmission Control Protocol (TCP).

Telnet was developed in 1968 beginning with RFC 15, extended in RFC 854, and standardized as Internet Engineering Task Force (IETF) Internet Standard STD 8, one of the first Internet standards.

Historically, Telnet provided access to a command-line interface (usually, of an operating system) on a remote host. Most network equipment and operating systems with a TCP/IP stack support a Telnet service for remote configuration (including systems based on Windows NT). However, because of serious security issues when using Telnet over an open network such as the Internet, its use for this purpose has waned significantly in favor of SSH.

The term *telnet* may also refer to the software that implements the client part of the protocol. Telnet client applications are available for virtually all computer platforms. *Telnet* is also used as a verb. *To telnet* means to establish a connection with the Telnet protocol, either with command line client or with a programmatic interface. For example, a common directive might be: "*To change your password, telnet to the server, log in and run the passwd command.*" Most often, a user will be *telnetting* to a Unix-like server system or a network device (such as a router) and obtaining a login prompt to a command line text interface or a character-based full-screen manager.

1 History and standards

Telnet is a client-server protocol, based on a reliable connection-oriented transport. Typically, this protocol is used to establish a connection to Transmission Control Protocol (TCP) port number 23, where a Telnet server application (telnetd) is listening. Telnet, however, predates TCP/IP and was originally run over Network Control Program (NCP) protocols.

Before March 5, 1973, Telnet was an ad hoc protocol with no official definition.[1] 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[2] with the publication of two NIC documents: Telnet Protocol Specification, NIC #15372, and Telnet Option Specifications, NIC #15373.

Because of negotiable options protocol architecture, many extensions were made for it, some of which have been adopted as Internet standards, 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)

2 Security

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 other people's servers, made encrypted alternatives necessary.

Experts in computer security, such as 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 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, switch, hub or gateway 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.
- Most implementations of Telnet have no authentication that would ensure communication is carried out between the two desired hosts and not intercepted in the middle.
- Several vulnerabilities have been discovered over the years in commonly used Telnet daemons.

These security-related shortcomings have seen the usage of the Telnet protocol drop rapidly, especially on the public Internet, in favor of the Secure Shell (SSH) protocol, first released in 1995. 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 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 (TLS) security and Simple Authentication and Security Layer (SASL) authentication that address the above issues. 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.

3 Telnet 5250

IBM 5250 or 3270 workstation emulation is supported via custom telnet clients, TN5250/TN3270, and IBM servers. Clients and servers designed to pass IBM 5250 data streams over Telnet generally do support SSL encryption, as SSH does not include 5250 emulation. Under OS/400, port 992 is the default port for secured telnet.

4 Telnet data

All data octets except 0xff are transmitted over Telnet as is. Therefore, a Telnet client application may also be used to establish an interactive raw TCP session, and it is commonly believed that such session which does not use the IAC (0xff, or 255 in decimal) is functionally identical. This is not the case, however, because there are other *network virtual terminal* (NVT) rules, such as the requirement for a bare carriage return character (CR, ASCII 13) to be followed by a NUL (ASCII 0) character, that distinguish the telnet protocol from raw TCP sessions. On the other hand, many systems now possess true raw TCP clients, such as netcat or socat on UNIX and PuTTY on Windows, which also can be used to manually "talk" to other services without specialized client software. Nevertheless, Telnet is still sometimes used in debugging network services such as SMTP, IRC, HTTP, FTP or POP3 servers, to issue commands to a server and examine the responses, but of all these protocols only FTP really uses Telnet data format.

Another difference of Telnet from a raw TCP session is that Telnet is not 8-bit clean by default. 8-bit mode may be negotiated, but high-bit-set octets may be garbled until this mode was requested, and it obviously will not be requested in non-Telnet connection. The 8-bit mode (so named *binary option*) is intended to transmit binary data, not characters though. 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,[3] but nothing is known about its actual software support.

5 Related RFCs

- RFC 137, TELNET protocol specification
- RFC 139, TELNET protocol specification
- RFC 854, TELNET protocol specification
- RFC 855, TELNET option specifications
- RFC 856, TELNET binary transmission
- RFC 857, TELNET echo option
- RFC 858, TELNET suppress Go Ahead option
- RFC 859, TELNET status option
- RFC 860, TELNET timing mark option
- RFC 861, TELNET extended options - list option
- RFC 885, Telnet end of record option
- RFC 1041, Telnet 3270 regime option
- RFC 1073, Telnet Window Size Option
- RFC 1079, Telnet terminal speed option
- RFC 1091, Telnet terminal-type option
- RFC 1096, Telnet X display location option
- RFC 1116, Telnet Linemode Option
- RFC 1123, Requirements for Internet Hosts - Application and Support
- RFC 1143, The Q Method of Implementing TELNET Option Negotiation
- RFC 1184, Telnet linemode option
- RFC 1205, 5250 Telnet interface
- RFC 1372, Telnet remote flow control option
- RFC 1572, Telnet Environment Option
- RFC 2217, Telnet Com Port Control Option
- RFC 2941, Telnet Authentication Option
- RFC 2942, Telnet Authentication: Kerberos Version 5

- RFC 2943, TELNET Authentication Using DSA
- RFC 2944, Telnet Authentication: SRP
- RFC 2946, Telnet Data Encryption Option
- RFC 4248, The telnet URI Scheme
- RFC 4777, IBM's iSeries Telnet Enhancements

6 Telnet clients

- PuTTY is a free, open-source SSH, Telnet, rlogin, and raw TCP client for Windows, Linux, and Unix.
- AbsoluteTelnet is a telnet client for Windows. It also supports SSH and SFTP,
- RUMBA (Terminal Emulator)
- Line Mode Browser, a command line web browser
- NCSA Telnet
- TeraTerm
- SecureCRT from Van Dyke Software
- ZOC Terminal
- SyncTERM BBS terminal program supporting Telnet, SSHv2, RLogin, Serial, Windows, *nix, and Mac OS X platforms, X/Y/ZMODEM and various BBS terminal emulations
- PowerTerm InterConnect from Ericom available for Windows, Mac OS X, Linux, Windows CE and supports 35 terminal emulation types including TN3270, TN5250, VT420, Wyse and others with SSH and SSL.
- Rtelnet is a SOCKS client version of Telnet, providing similar functionality of telnet to those hosts which are behind firewall and NAT.
- Inetutils includes a telnet client and server and is installed by default on many GNU/Linux distributions.

7 See also

- Virtual terminal
- Reverse telnet
- HyTelnet
- Kermit
- SSH

8 References

[1] RFC 318 - documentation of old ad hoc telnet protocol

[2] RFC 495 - Announcement of Telnet protocol

[3] RFC 2066: TELNET CHARSET Option

9 External links

- Telnet Options - The official list of assigned option numbers at iana.org
- Telnet Interactions Described as a Sequence Diagram
- Telnet protocol description, with NVT reference
- Microsoft TechNet:Telnet commands
- TELNET: The Mother of All (Application) Protocols
- Troubleshoot Telnet Errors in Windows Operating System

10 Text and image sources, contributors, and licenses

10.1 Text

- **Telnet** *Source:* https://en.wikipedia.org/wiki/Telnet?oldid=670452975 *Contributors:* Uriyan, Robert Merkel, Tarquin, Drj, Youssefsan, Vaganyik, Aldie, Mjb, Hephaestos, Bdesham, Kwertii, Liftarn, Ixfd64, Tregoweth, Ahoerstemeier, Ronz, Glenn, Nikai, Kwekubo, HPA, Xanthine, Fuzheado, WhisperToMe, Furrykef, Lensi, Spikey, Betterworld, Joy, Sena, Mrjeff, AlexPlank, Robbot, Lambda, Pigsonthewing, RedWolf, Nurg, Romanm, Kwi, MaXim, Victor, Buster2058, Giftlite, Laudaka, Joaopaulo1511, Brian Kendig, Mark Richards, Fleminra, Jdavidb, Devisualize~enwiki, Yekrats, AlistairMcMillan, Taak, Isidore, Chowbok, Alexf, Antandrus, Bumm13, Astronouth7303, JTN, RossPatterson, Discospinster, Marxmax~enwiki, Horkana, Sundaedeluxe, Project2501a, Richard W.M. Jones, Sietse Snel, Femto, Nigelj, John Vandenberg, Polluks, A Wikipedia user from Minnesota, Wrs1864, Davidsmind, SPUI, Wayfarer, Pion, FtWashGuy, Stephan Leeds, Suruena, Tedp, Drat, Sleigh, Kinema, Rzelnik, Saxifrage, Aadnk, Feezo, Woohookitty, ^demon, Frungi, Meneth, CharlesC, Elvarg, Pfalstad, Atari2600tim, Ashmoo, Dpr, Pmj, Koavf, ElKevbo, Wfryer, Sango123, Yamamoto Ichiro, Jasoneth, FlaBot, Carlos Barreto, Vclaw, Nivix, Ewlyahoocom, Sstrader, TeaDrinker, Chobot, DVdm, YurikBot, Borgx, RussBot, Peter S., Taejo, Wiki alf, Smartyhall, KEK, Mad Max, Julienlecomte, Alex43223, CrazyLegsKC, DeadEyeArrow, Anwynd, Gtdp, Mateo LeFou, Abune, Skedaddle, Ed de Jonge, Pasi, Chris Chittleborough, SmackBot, Michael Meyling, Classicfilms, Incnis Mrsi, David.Mestel, Phorteetoo, MeiStone, KocjoBot~enwiki, Sydius, BiT, Grawity, Lordandmaker, BenAveling, Henrique Moreira~enwiki, EdgeOfEpsilon, Omniplex, Stormchaser, Zordrac, Awh, Maulattu, Addshore, UU, Anoopkn, Only, Mroblivious1bmf, Daniel.Cardenas, TenPoundHammer, SashatoBot, Simen 88, Beard0, Infofarmer, Ehheh, Dicklyon, Doczilla, Behemoth2302, Udtrivedi, Young Zaphod, NEMT, Bauani, JoeBot, Beno1000, V0rt3x, Courcelles, Frank Lofaro Jr., Kotepho, FatalError, Unixguy, CmdrObot, Foice, DanielRigal, INVERTED, Neelix, Equendil, Phatom87, Jjclarkson, Cydebot, Kanags, Rob.desbois, UncleBubba, Doug Weller, Juansempere, DumbBOT, Thijs!bot, Epbr123, Daniel, Andyjsmith, Jdm64, Mr.Blonde, Druiloor, I already forgot, Mentifisto, AntiVandalBot, Shirt58, Canadian-Bacon, MikeLynch, Harryzilber, Tonyrocks922, Bonze~enwiki, PhilKnight, Enjoi4586, Benstown, Magioladitis, VoABot II, Janadore, Tedickey, Tremilux, Bzero, Email4mobile, Rich257, KJRehberg, Rswindell, Arsanmkt, Gaigeb, Gwern, DancingPenguin, MartinBot, Bpence, Boston, Francis Tyers, TinaSDCE, EdBever, Tgeairn, J.delanoy, Mange01, Bogey97, Tisteca, Vanished user 342562, Laurusnobilis, Wandering Ghost, Thomas Larsen, AntiSpamBot, SJP, Gfis, Spellcast, VolkovBot, AlnoktaBOT, Epo1968, Kyle the bot, TXiKiBoT, Jkstark, Jjohn555, Clarince63, Bugone, NodnarbLlad, Haseo9999, Ceranthor, Entbark, Kbrose, Nubiatech, Flavinhu, Oxymoron83, Lightmouse, Alex.muller, Millstream3, Brentes, ThomasLB, MarkMLl, Smashville, ClueBot, Sanjayk gupta, Badger Drink, Lawrence Cohen, Edgesurge, Pitvipper, PixelBot, Vanisheduser12345, Awisch, Lartoven, Lkedziora, Andmott, Real Deuce, Ottawa4ever, Farimah~enwiki, Russ1231, XLinkBot, BodhisattvaBot, Rror, Cardatron, BDFun, Bandoche, Addbot, Some jerk on the Internet, Mabdul, MrOllie, Chamal N, Favonian, SamatBot, Bfigura's puppy, Slgcat, Legobot, Legobot II, II MusLiM HyBRiD II, Amble, Nallimbot, AnomieBOT, Jim1138, Sz-iwbot, Zadneram, Capricorn42, Zicko1, DutchmanInDisguise, Shadowjams, Chaheel Riens, Manny1208, Datakid1100, Surv1v4l1st, Mark Renier, Thoughtful Goose, Flint McRae, 231O, Alexihelligar, Reconsider the static, TobeBot, ItsZippy, Shaywalters, Reaper Eternal, Thomassteinke, Onel5969, EmausBot, WikitanvirBot, Mayazcherquoi, Wikipelli, Erpert, ProbitSoftware, Mpotter27, Orange Suede Sofa, Knarrff, ClueBot NG, Nimiew, Satellizer, Braincricket, Calabe1992, Ramaksoud2000, Island Monkey, Ashishdhenge, Tarcil, Joydeep, Vaijayanth, Ytic nam, M4r51n, Dr Dinosaur IV, I am One of Many, Jamesmcmahon0, EternalFlare, ArmbrustBot, Dannyniu, Lesser Cartographies, Jianhui67, DeeBoFour20, Abbotn, Bawari, Shaisn, Liadbrady and Anonymous: 423

10.2 Images

- **File:Question_book-new.svg** *Source:* https://upload.wikimedia.org/wikipedia/en/9/99/Question_book-new.svg *License:* Cc-by-sa-3.0 *Contributors:*
  Created from scratch in Adobe Illustrator. Based on Image:Question book.png created by User:Equazcion *Original artist:* Tkgd2007

10.3 Content license

- Creative Commons Attribution-Share Alike 3.0