TELNET

Telnet is the short form for TErminal NETwork. It basically a TCP/IP protocol that is used for virtual terminal services and was mainly proposed by the International Organization for Standards (ISO). It is a simple command line tool that runs on your computer and allows you to send commands remotely to a server and administer that server just as if you were sitting in front of it.

So, when you connect remotely to a server using telnet you would just use type commands with the keyboard to tell that server what to do. So, you can use those commands to run programs, create folders, delete files, create files, transfer files, browse directories, start or stop services and so on. You can do pretty much everything even if you are thousand miles away from that particular server. And in addition to communicating with servers, telnet is also used to manage and configure other networking devices such as routers and switches. It can also be used to check if ports are opened or closed on a server. Telnet is used with operating system such as windows and MacOS, but largely used on Linux and Unix system.

As mentioned before, Telnet is command line tool. Therefore, there is no graphical user interface. It’s just a very simple, text-oriented utility that will run on a computer. As a matter of fact, you do not even have to have a computer to run telnet! A simple dumb terminal can be used, and all the commands are sent using a keyboard. Because it only sends commands and not graphics, telnet is very fast.

Now telnet was developed way back in 1969 and because it was developed prior to the internet, security was not really an issue. So, with telnet, all the commands are sent in clear text, so there is no encryption.

So, if we were to use telnet today to communicate with server over the internet, someone can easily eavesdrop and grab any sensitive data, that you are sending to that server such as usernames and password. Because of the lack of encryption, telnet is outdated today and should not be used over public internet.

But it is still being used today in local are networks and not over the internet. It can also be used if you are working with older equipments that cannot support modern protocols like SSH.

The Telnet was mainly designed at the time when most O.S operate in time sharing environment (Method of operation in which multiple users with different program interact nearly simultaneously with the CPU of a large-scale computer). And in this type of environment, a large computer can support multiple users.

Telnet makes use of only one TCP/IP connection and works on port number 23.

Logging

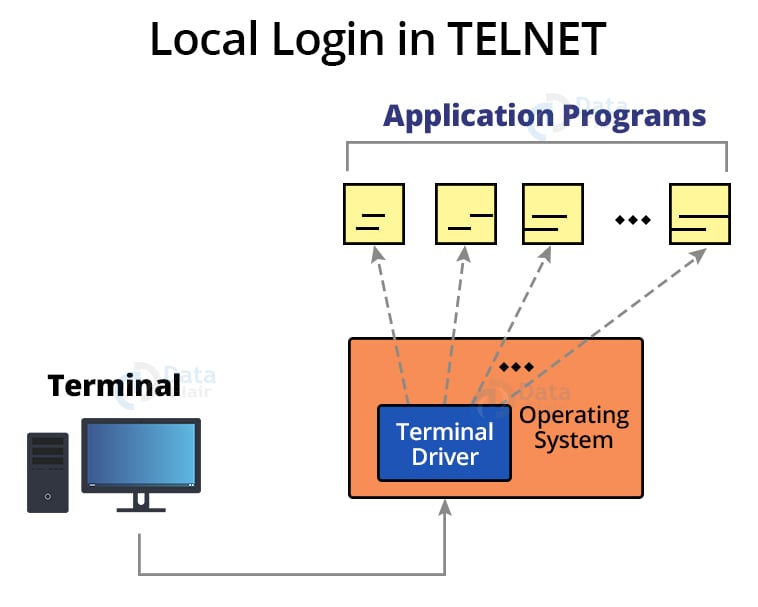
In the time-sharing environment, the users are a part of the system having some rights in order to access the resources. It is important to note that each user is given an identification along with the password. This user identification mainly indicates that this user is part of the system.

In order to access the system, the user logs in to the system by the user-id. The system also includes password checking in order to prevent any unauthorized access to the resources of a system.

The logging process can further be categorized into 2 parts:

1. Local Log-In
2. Remote Log-In

Local Log-In

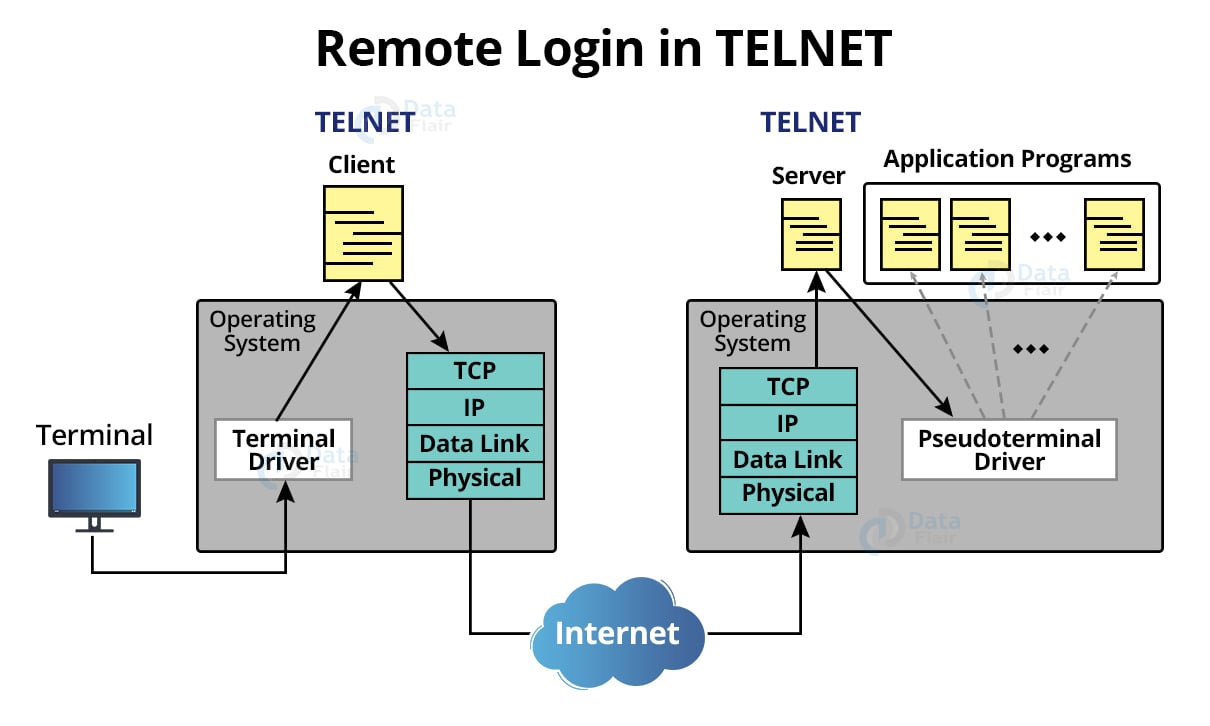


Step 1: Once the user types at the terminal, the keystroke are accepted by the terminal driver.

Step 2: The terminal driver passes the characters to the OS.

Step 3: The OS in turn, interprets the combination of characters and invokes the desired application program or utility.

Remote Log-In



When a user wants to access an application program or utility located on a remote machine, one performs remote log-in, the telnet client/server program mainly comes to use.

Step 1: User sends the keystrokes to the terminal driver, where the local OS accepts the characters but does not interpret them

Step 2: The characters are sent to Telnet Client, which transforms the characters into a universal character set called a network virtual terminal (NVT) characters and delivers them to the local TCP/IP protocol stack.

Step 3: The commands or text in NVT form, travel through the internet and arrive at the TCP/IP stack at the remote machine.

Step 4: However, the characters cannot be directly passed to the OS, because the remote O.S is not designed to receive the characters from a telnet server. It is designed to receive characters from a terminal driver.

Step 5: The solution? It is to add a piece of software called a pseudo terminal driver which pretends that the characters are coming from a terminal. The O.S then passes the character to the appropriate application program.

Network Virtual Terminal

The mechanism to access a remote computer is complex. This is because every computer and its O.S accepts a special combination of characters as tokens. Example – The end of file token in a computer running the DOS (Disk O.S) is ctrl+Z, while the UNIX O.S recognizes ctrl+d.

We are dealing with heterogenous system. If we want to access any remote computer in the world, we must first know what type of computer we will be connected to and we must also install the specific terminal emulator used by that computer.

Telnet solves this problem by defining a universal interface called the Network Virtual Terminal (NVT) character set.

Via this interface, the client Telnet translates character (data or commands) that come from the local terminal into NVT form and deliver them to the N/W. The server telnet, on the other hand, translates data and commands from NVT form into the form acceptable by the remote computer.

* The Network Virtual Terminal (NVT) primarily employs two sets of characters: one for data and another for control.
* It is an 8-bit character set for data, with the 7 lowest-order bits identical to ASCII and the highest bit set to 0.
* It uses an 8-bit bit character set to communicate control characters between the computers, with the highest-order bit set to 1.
* For sending data and control characters the TELNET makes use of the same connection by just inserting control characters into the data stream.
* Each control character is preceded by the Special Control character, which is popularly known as Interpret as Control, for separating the data characters from the control characters (IAC).

Example:

A user wants a server to display a file (file1) on a remote server.

* So we type – Catfile1

But suppose the name of the file has been mistyped (file a instead of file 1). The user then uses the backspace key to correct this mistake.

* Catfilea<backspace>1

However, in default implementation of telnet, the user cannot edit locally, the editing is done at the remote server. The backspace character is translated into two remote characters(IAC EC), which are embedded in the data and sent to the remote server.

Representation of the types text by the user.


Advantages

1. Telnet allows remote access to someone else computer system.
2. As telnet makes the user of plain text, thus this allows the user for more access with fewer problem in data transmissions
3. Telnet is universal as it can be used on any computer, even the oldest system can easily connect to the newer machines while both having different versions of the O.S

Disadvantages:

1. As no graphical user interface, it might be difficult for some users to get the hang of it.
2. Since there is no concept of encryption, it is therefore not considered as a secured method.

Modes of operation:

Default Mode:

* When no other modes are called, this mode is utilized
* In this mode, the client performs echoing.
* In this mode, the user enters a character, and the client repeats it on the screen but does not send it until the entire line is done.

Character Mode:

* Each character entered in this mode is transmitted to the server by the client.
* In this mode, the server typically repeats the character back to the client’s screen.

Line Mode:

* Line editing, such as echoing and character deleting, is done on the client side.
* The entire line will be sent to the server by the client.

Now because for obvious reason we cannot use Telnet, another protocol which is much more secured came into picture – SSH. Secure Shell

Secure shell works exactly like Telnet but with additional security.

SSH, also known as Secure Shell or Secure Socket Shell, is a network protocol that gives users, particularly system administrators, a secure way to access a computer over an unsecured network.

The encryption methods used are:

1. Symmetrical Encryption
2. Asymmetrical Encryption
3. Hashing

Symmetric key Encryption

In this technique,

* Both sender and receiver uses a common key to encrypt and decrypt the message.
* This secret key is known only to the sender and to the receiver.
* It is also called as **secret key cryptography**.

## **Working-**

The message exchange using symmetric key cryptography involves the following steps-

Process of Symmetric Key Encryption


* Before starting the communication, sender and receiver shares the secret key.
* This secret key is shared through some external means.
* At sender side, sender encrypts the message using his copy of the key.
* The cipher text is then sent to the receiver over the communication channel.
* At receiver side, receiver decrypts the cipher text using his copy of the key.
* After decryption, the message converts back into readable format.

## **Important Points-**

In symmetric key cryptography,

* Both sender and receiver uses the same key.
* Sender encrypts the message using his copy of the key.
* Receiver decrypts the message using his copy of the key.
* The key must not be known to anyone else other than sender and receiver.
* If the secret key is known to any intruder, he could decrypt the message.
* This cryptography technique is called as **symmetric key cryptography**.
* It is because both sender and receiver use the same key on their sides.
* This cryptography technique is called as **secret key cryptography**.
* It is because the key has to be kept secret between the sender and receiver.

## **Asymmetric Key Encryption**

## In this technique,

* Sender and receiver use different keys to encrypt and decrypt the message.
* It is called so because sender and receiver use different keys.
* It is also called as **public key cryptography**.

## **Working-**

The message exchange using public key cryptography involves the following steps-

Process of Asymmetric Key Encryption


## **Step-01:**

At sender side,

* Sender encrypts the message using receiver’s public key.
* The public key of receiver is publicly available and known to everyone.
* Encryption converts the message into a cipher text.
* This cipher text can be decrypted only using the receiver’s private key.

## **Step-02:**

* The cipher text is sent to the receiver over the communication channel.

## **Step-03:**

At receiver side,

* Receiver decrypts the cipher text using his private key.
* The private key of the receiver is known only to the receiver.
* Using the public key, it is not possible for anyone to determine the receiver’s private key.
* After decryption, cipher text converts back into a readable format.

Hashing:

Hashing is the process of transforming any given key or a string of characters into another value. It is an algorithm that uses mathematical function with the help of which it garbles data and makes it unreadable.