CC BY NC ND

TELNET Communication

It is a form of remote control to manage mainframe computers from distant terminals. It is interactive text-oriented communication. Using Telnet, the remote user can log into the remote machine. For telnet communication, TCP connection shall be established. Telnet uses port 23 to log into the remote machine. In the OSI model, Telnet lies in the Application layer.

On March 5, 1973, a Telnet protocol standard was defined at UCLA with the publication of two NIC documents: Telnet Protocol Specification, NIC 15372, and Telnet Option Specifications, NIC 15373.

Essentially, it uses an 8-bit channel to exchange 7-bit ASCII data. In TELNET, This 7-bit ASCII data can be classified as commands or user data. If the Most Significant Bit is 1, this means that this is a command sequence. Therefore ASCII characters with decimal value between 0 and 127 are handled as user data. Characters between 128 and 255 are interpreted as command sequence.

User data characters are further handled as printable characters (from 33 to 127) or control characters (from 0 to 32).

TELNET Command Structure

The following sequence represents how a TELNET command can be sent

```
IAC <command code> [option]
```

Where *IAC* is a special command with ASCII code 0xFF is used to start a command sequence. The following is a sample of defined commands for the TELNET

Name	Code in Dec	Code in Hex	Description
SE	240	0xF0	End of subnegotiation parameters
NOP	241	0xF1	No Operation
DM	242	0xF2	Data Mark: indicates the position of sync event within the data stream. This should always be accompanied by a TCP urgent notification
BRK	243	0xF3	Break: indicates that the break or attention key was hit
IP	244	0xF4	Suspend Interrupt or abort the process to which the NVT is connected
AO	245	0xF5	Abort Output: allows the current process to run to completion but does not send its output to the user
AYT	246	0xF6	Are You There: send back to the NVT some visible evidence that the AYT was received
EC	247	0xF7	Erase Character: the receiver should delete the last preceding undeleted character from the data stream
EL	248	0xF8	Erase Line: delete characters from the data stream back to but not including the previous CRLF
GA	249	0xF9	Go Ahead: under certain circumstances used to tell the other end that it can transmit
SB	250	0xFA	Subnegotiation Begin: with the indicated option that follows
WILL	251	0xFB	The sender wants to enable the option itself
WONT	252	0xFC	The sender wants to diable the option itself
DO	253	0xFD	The sender wants the receiver to enable the option
DONT	254	0xFE	The sender wants the receiver to disable the option
IAC	255	0xFF	Interpret what follows as a command

Table 1: TELNET Commands

BY NC ND

As an example, a terminal device may send the command

```
IAC DO 24
```

The responder device shall reply with the following command if it is ready or successful

```
IAC WILL 24
```

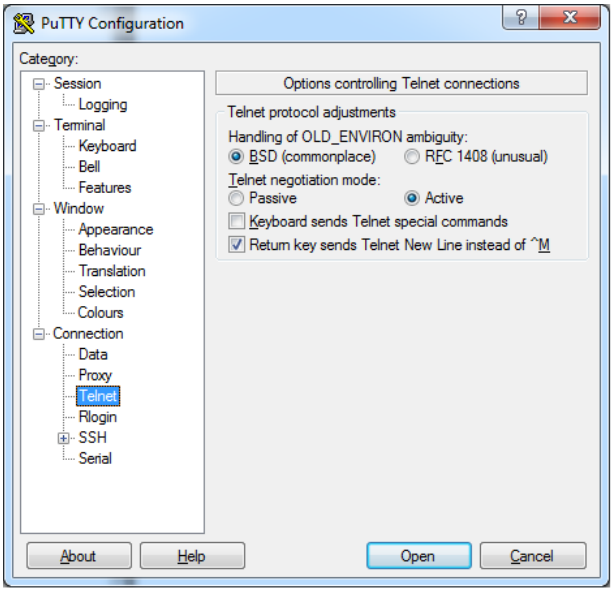
Or if it is not ready, it can refuse the command by replying

```
IAC WONT 24
```

Telnet Software

Some ready and free software can be used to initiate TELNET connection between two machines. In linux telnet package can be used for that purpose. In Windows, there are several free software for that for example PacketSender and PuTTy. In the following shots, telnet settings in PuTTY is described .

Use the following default settings in PuTTY:



To start communication, click 'Open'