Virtual terminals

Remote access with telnet or SSH video

.

Telnet

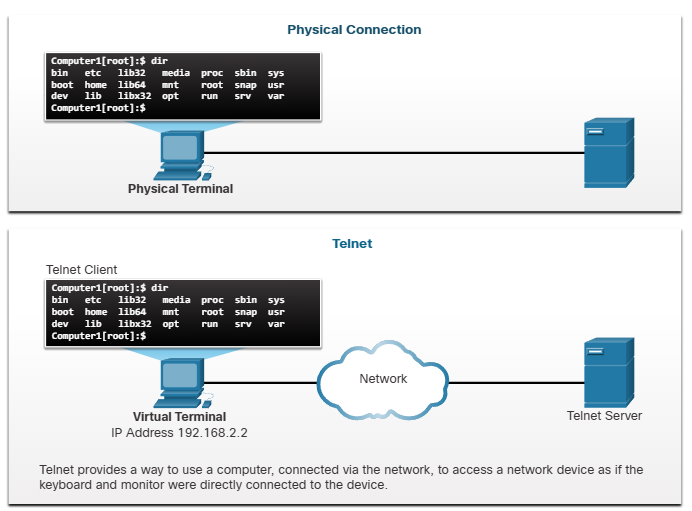
it dates back to 1970s and is among the oldest of the application layer protocols and services in the TCP/IP suite.

It provides a standard method of emulating text-based terminal devices over the data network.

Both the protocol itself and the client software that implements the protocol are commonly referred to as Telnet. **Telnet servers listen for client requests on TCP port 23**

Appropriately enough, **a connection using telnet is called a virtual terminal (vty) session, or connection.**

**Rather than using a physical device to connect to the server, telnet uses software to create a virtual device that provides the same features of a terminal session with access to the servers command line interface (CLI)**



\

Security issues with telnet

**After a telnet connection is established, users can perform any authorized function on the server, just as if they were using a command line session on the server itself.**

If authorized, they can start and stop processes, configure the device, and even shut down the system.

**Although the telnet protocol can require a user to login**, **it does not support transporting encrypted data. All data is exchanged as plaintext across the network**

**The secure shell (SSH) protocol** offers an alternate and secure method for server access.

SSH provides the structure for secure remote login and other secure network services.

It also provides **stronger authentication than telnet and supports transporting session data using encryption**.

As a best practice, network professionals should always use SSH in place of telnet.

