

# Protocole TELNET



*NISRINE BAKHOUC*

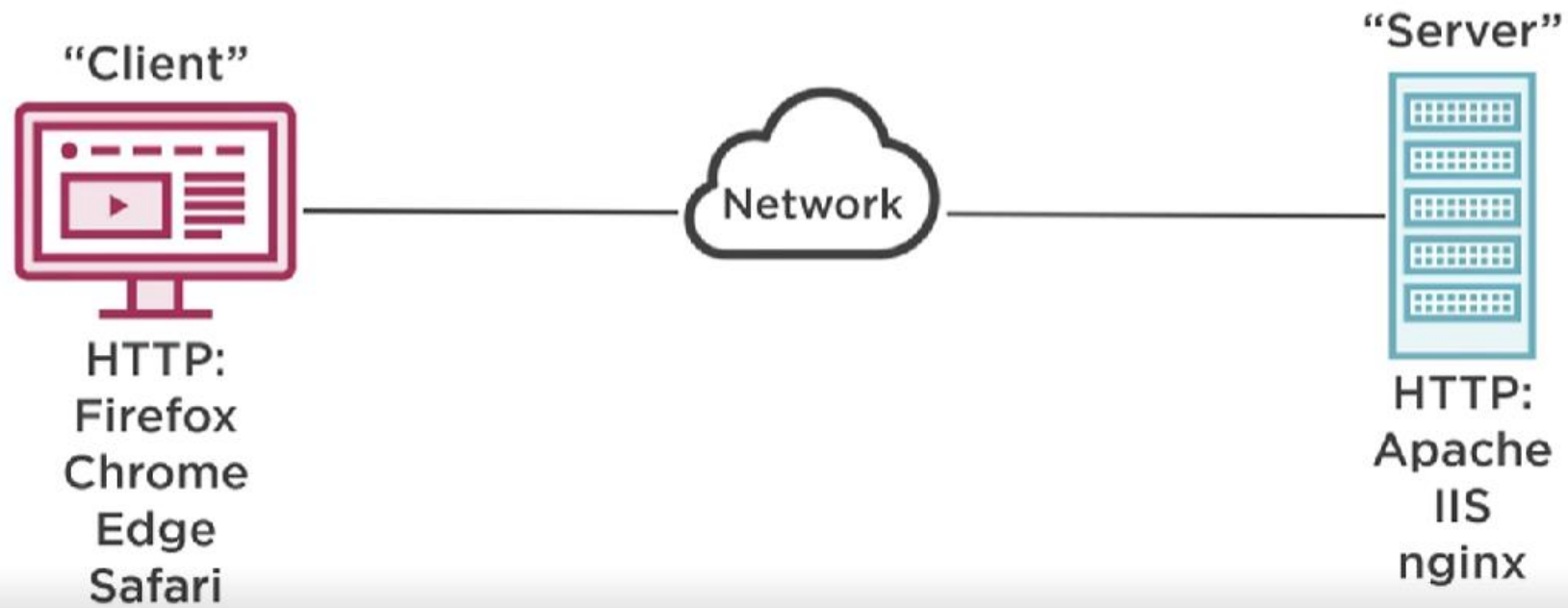
*Encadree par:  
Pr.Mehdi Moukhafi*



# *Plan*

- Protocole client serveur
- histoire
- Definition de telnet
- Comment fonctionne telnet
- Utilisation
- Les avantages et les inconvenient du protocole telnet
- xinetd
- Installation et configuration de telnet

Exemple:



## Protocole client serveur :

Le protocole ou environnement **client–serveur** désigne un mode de transaction (souvent à travers un réseau) entre plusieurs programmes ou processus : l'un, qualifié de **client**, envoie des requêtes ; l'autre, qualifié de **serveur**, attend les requêtes des clients et y répond. Le serveur offre ici un **service** au client.

---

- **Client** :il envoie des requêtes au serveur ;  
il attend et reçoit les réponses du serveur.
- **Serveur**:il est à l'écoute, prêt à répondre aux requêtes envoyées par des clients ;  
dès qu'une requête lui parvient, il la traite et envoie une réponse.

Le client et le serveur doivent bien sûr utiliser le même protocole de communication. au niveau de la **couche transport** du **modèle OSI**.

---

## *La motivation pour le développement de Telnet*

Deux problèmes :

**La première** était que si vous aviez plusieurs ordinateurs différents dans une organisation, chaque utilisateur aurait besoin d'un terminal distinct pour accéder à chaque ordinateur qu'il devait utiliser. C'était cher et inefficace;

**Le deuxième** problème, et peut-être le plus important, était la difficulté d'autoriser un utilisateur à accéder à une machine distante et à l'utiliser. La seule méthode à l'époque pour y parvenir était d'installer un circuit de données dédié de l'ordinateur à l'utilisateur, pour connecter le terminal de l'utilisateur à la machine distante. Là encore, chaque circuit ne permettrait l'accès qu'à une seule machine. Chaque combinaison d'utilisateur et d'ordinateur aurait nécessité l'installation et la maintenance d'un circuit séparé et coûteux.

---

## ***Historique Telnet***

Telnet a été le premier protocole d'application démontré sur [ARPAnet](#), en 1969.

Le premier RFC définissant spécifiquement Telnet était [RFC 97](#), publié en février 1971.

Le développement de Telnet s'est poursuivi tout au long des années 1970, avec un certain nombre de différentes RFC consacrées aux révisions du protocole et aux discussions sur les questions qui s'y rapportent.

//\*\*\* Il a fallu de nombreuses années pour affiner Telnet et résoudre toutes les difficultés associées à son développement.\* /

La version finale du protocole, [Telnet Protocol Specification](#), a été publiée en tant que [RFC 854](#) en mai 1983. Au fil des ans, d'autres RFC ont été publiées pour clarifier l'utilisation du protocole et résoudre divers problèmes tels que l'authentification. Il existe également un certain nombre d'autres RFC qui définissent les options Telnet

\*\*RFC: [Request for comments](#) sont un ensemble de documents qui font référence auprès de la Communauté Internet et qui décrivent, spécifient, aident à l'implémentation, standardisent de la majorité des normes, standards, technologies et protocoles liés à Internet et aux réseaux en général.

n'importe qui peut écrire une RFC et la soumettre à l'IETF

---

## Definition:

**Telnet** *Teletype Network* est un **protocole client-serveur** basé sur l'échange de données via des connexions TCP.

Le protocole permet le contrôle d'ordinateurs à distance grâce à des entrées et sorties textuelles. Pour ce faire, une **connexion client-serveur** est établie par défaut en utilisant le **protocole TCP** et le **port TCP 23** : le périphérique agit comme un serveur et attend les commandes.

---



Créé en **1969**,

telnet est un moyen de communication très généraliste et bi-directionnel.

Il appartient à la couche application du **modèle OSI**.

décrit par le **RFC 854 ET RFC 855**

Il est normalisé par **IETF** (*Internet Engineering Task Force*).

**IETF**:organisation Mondiale de bénévoles collaborant pour concevoir des normes qui fournissent l'infrastructure pour

L'innovation sur internet

---

Le protocole repose sur trois concepts principaux :

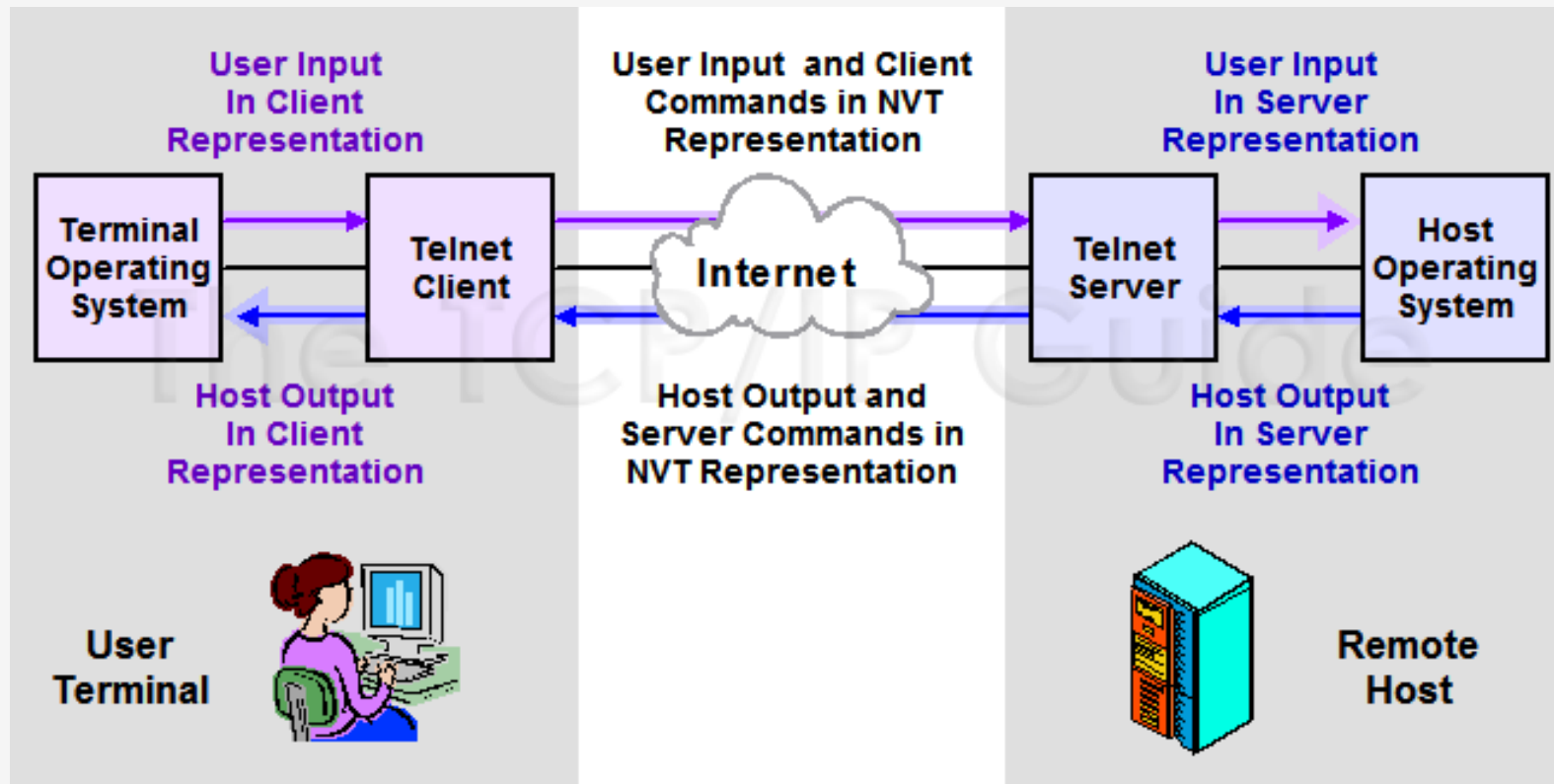
1. **The Network Virtual Terminal (NVT)**
  2. **Options and Option Negotiation** : Telnet définit un riche ensemble d'options et un mécanisme par lequel un client et un serveur Telnet peuvent négocier leur utilisation. Si le client et le serveur s'accordent sur l'utilisation d'une option, celle-ci peut être activée .
  3. **Symmetric Operation** : bien que Telnet soit un protocole client/serveur, il est spécifiquement conçu pour ne pas faire d'hypothèses sur la nature du logiciel client et serveur. Une fois qu'une session Telnet est établie, ils peuvent chacun envoyer et recevoir des données sur un pied d'égalité. Ils peuvent également initier chacun la négociation des options. Cela rend le protocole extrêmement flexible et a conduit à son utilisation dans une variété d'endroits,
-

- NVT (Network Virtual Terminal) est un terminal virtuel dans TELNET qui a une structure fondamentale partagée par de nombreux types différents de terminaux réels.
- Les clients et serveurs TELNET envoient des données, des commandes et la sortie du serveur à l'aide d'un type de terminal virtuel appelé NVT, plutôt qu'une variété de types de terminaux pour différents systèmes d'exploitation (Network Virtual Terminal), car les systèmes sont aujourd'hui hétérogènes.
- NVT (Network Virtual Terminal) a été créé pour rendre viable la communication entre différents types de terminaux avec différents systèmes d'exploitation.

Il fonctionne comme suit et est également représenté dans la figure ci-dessus :

---

Le **client TELNET** convertit les caractères du terminal local au format NVT puis les envoie sur le réseau.



le **serveur TELNET** convertit les données et les commandes au format NVT dans un format que les ordinateurs distants peuvent comprendre.

## *Utilisation:*

- Se connecter a des serveurs telnet
  - Une commande pour tester des serveurs pour etablir une connection tcp interactive avec d'autre services tq SMPT,HTTP... en utilisant le port du protocole
  - Configurer des commutateur , des routeur , des serveurs d'impression,etc
-

*AVANTAGES* :

- *Protocole multiplateforme*
- *Rapide ( no GUI)*

*INCONVENIENTS* :

- *un protocole de transfert de données non sécurisé (Clear text)*

---

# xinetd

**xinetd** est l'abréviation de *extended internet services daemon*, il remplace avantageusement **inetd**

**Xinetd** est un **démon** open source qui gère les connexions Internet sur de nombreux **serveurs** Unix et de type Unix modernes . Il offre une sécurité améliorée par rapport au démon **inetd** traditionnel et a remplacé inetd dans la plupart des versions modernes de **Linux**, **BSD** et **macOS**.

Il écoute le **trafic** réseau entrant et lance le service approprié, tel que FTP , HTTP ou UDP, pour gérer le trafic..

Dans l'absolu, inetd et xinetd ont le même rôle, à savoir de piloter l'accès à un ou plusieurs services réseaux. Ils agissent comme une standardiste. Ils reçoivent des requêtes de clients, extérieurs pour la plupart, qui demandent un accès à un service réseau déterminé (ex : ftp, telnet, ssh...). Le super démon va, en fonction des instructions qu'on lui aura données (fichiers de configuration) transmettre ou rejeter l'appel.

Sous Unix et Linux, le service est fourni par ce que l'on appelle un démon un **démon** est un programme qui s'exécute en arrière-plan sans nécessiter aucune interaction de l'utilisateur.

Par exemple, **httpd** ( [Hypertext Transfer Protocol](#) Daemon) s'exécute en tant que processus d'arrière-plan sur de nombreux serveurs Web, y compris ceux créés par Apache . Httpd attend et répond aux requêtes effectuées via HTTP, en fournissant des pages Web et d'autres fichiers selon les besoins

---



Telnet est considéré comme non sécurisé car il transfère toutes les données en texte clair sur le réseau, mot de passe compris . Ce qui signifie que si un utilisateur sniffer un réseau, il est très possible qu'il puisse saisir votre nom d' utilisateur et votre mot de passe au fur et à mesure de leur transmission.

Des protocoles chiffrés comme SSH ont été développés pour fournir un accès distant remplaçant Telnet et dont l'interception ne fournit aucune donnée utilisable à un éventuel espion du net

---

# *Reference:*

- <https://www.techno-science.net>
  - <https://www.ionos.fr/>
  - <https://www.pluralsight.com>
  - <https://fr.wikipedia.org>
  - <https://www.javatpoint.com>
  - <https://geekflare.com>
  - <https://www.funix.org/>
  - <https://waytolearnx.com/>
  - <https://jean-luc-massat.pedaweb.univ-amu.fr/>
-