Proposed By :
- **M.Muzzamal**
- **Imran Ali**

Date :
31 Dec, 2024

Group:
Group#09

Computer Networking

Remote Access with Telnet
(Configure Telnet for Remote Access to Network Devices)

Submitted to:
Mam Shehrish

Semester Project Report: Remote Access with Telnet

Table of Contents

- Test Network Connectivity

10. Network and analysis

- Network performance evolution
- Achievements
- Summary of the project
- Key learnings

11. Uses of Telnet

12. Advantages and disadvantages

13. Tools and Resources

- Learning outcomes

14. Conclusion

Introduction to TELNET

TELNET stands for **Teletype Network**. It is a client/server application protocol that provides access to virtual terminals of remote systems on local area networks or the Internet. The local computer uses a telnet client program and the remote computers use a telnet server program. In this article, we will discuss every point about TELNET.

Objective:

This network is aimed at showing how to configure and use remote access using Telnet in a multi-subnet environment. With three routers, three switches, and nine PCs, the network is capable of communication between subnets, and the management and monitoring of routers are possible over the internet. This network setup brings out some key concepts in networking, including IP addressing, routing, and Telnet configuration to provide centralized control and troubleshooting capabilities. The project puts forward the significance of remote management in modern networks and provides a scalable and practical solution for real-world applications.

History of TELNET

The Telnet protocol originated in the late 1960s, it was created to provide remote terminal access and control over mainframes and minicomputers. Initially, it was designed to be a simple and secure method of connecting to a remote system. This protocol allowed users to access remote computers using a terminal or command-line interface. Over time, Telnet's use has diminished due to security concerns, and alternatives like SSH are now preferred for secure remote management.

Scope of this network

- **Telnet Setup and Configuration**: Establish and configure Telnet for secure remote network access.
- **Design of Digital Logic Circuits**: Create and analyze circuits using basic gates and combinational logic.
- **Combinational Circuit Optimization**: Optimize circuits like adders, subtractors, and multiplexers for efficiency.
- **Network Security Implementation**: Secure Telnet connections and the network with encryption, authentication, and access control.
- **Integration of Network and Digital Systems**: Ensure smooth integration of digital logic systems with the network for reliable communication and data processing.

Requirement

Hardware requirement:

- **Client-side devices:** PC, Laptop, or any device for running telnet client application.
- **Server-**side devices: A server that supports telnet services.

Software requirement:

- **Network Configuration Tool**: Cisco Packet Tracer or GNS3 for network simulation (or a real network device for hands-on implementation).
- **Operating System**: Windows/Linux for PC.

Basic Knowledge:

- Understanding of basic networking concepts such as IP addressing, sub-netting, routing, and switch configuration.
- Familiarity with **Cisco's IOS command-line interface.**

Network Design and Topology

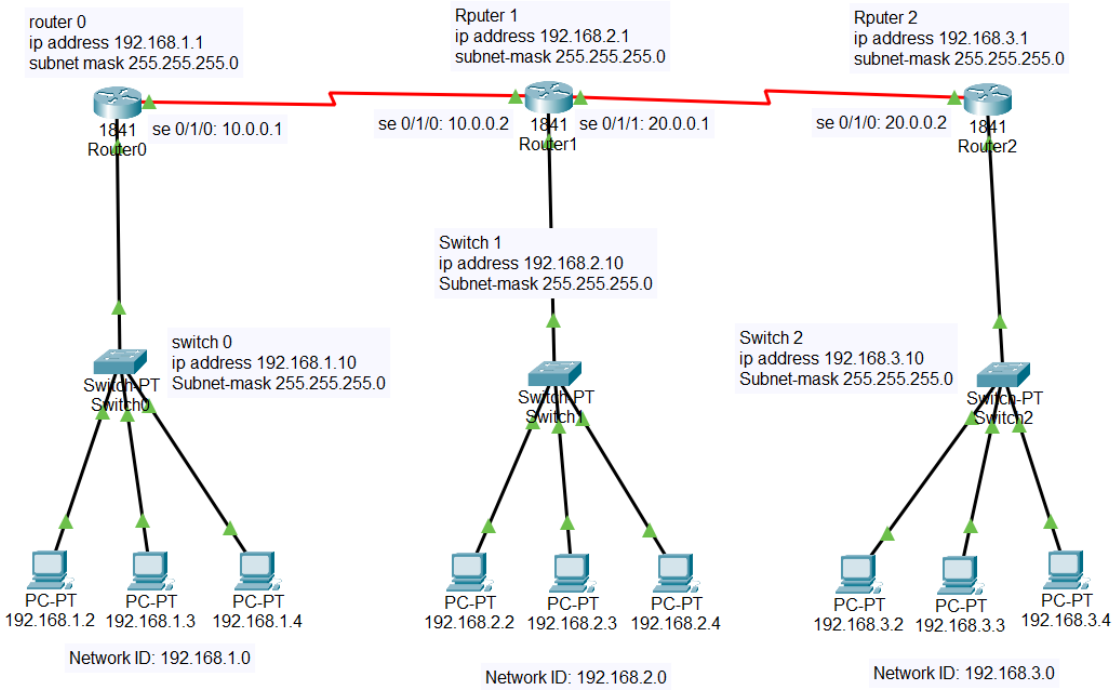
Logic Topology:

The network consists of three subnets connected via routers, forming a hierarchical design.

Physical Topology:

Each router connects to a switch, and each switch connects to three PCs within the subnet. Serial connections are used between the routers.

Structure of Network (Telnet)



Logging in TELNET

The logging process can be further categorized into two parts:

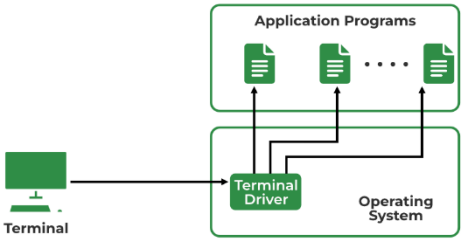
- Local Login
- Remote Login

1. Local Login

Whenever a user logs into its local system, it is known as local login.

The Procedure of Local Login

- Keystrokes are accepted by the terminal driver when the user types at the terminal.
- Terminal Driver passes these characters to OS.
- Now, OS validates the combination of characters and opens the required application.

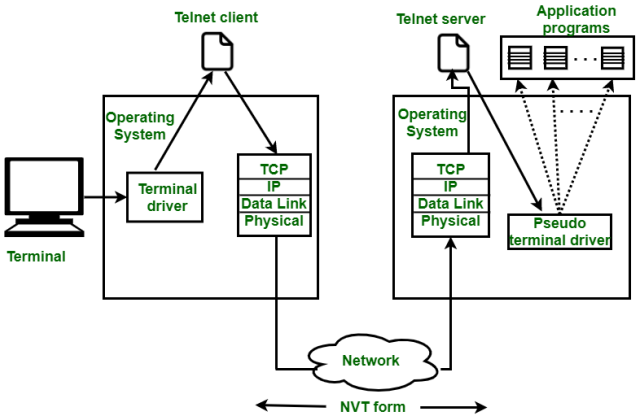


2. Remote Login

Remote login is a process in which users can log in to a remote site i.e. computer and use services that are available on the remote computer. With the help of remote login, a user is able to understand the result of transferring the result of processing from the remote computer to the local computer.

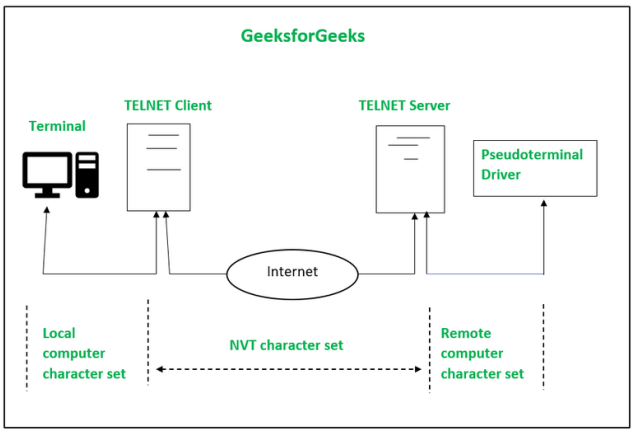
The Procedure of Remote Login

- User types characters, which are accepted by the local operating system.
- Converts characters into Network Virtual Terminal (NVT) format and sends them via TCP/IP.
- NVT characters travel through the internet to the remote computer's TCP/IP stack.
- Converts NVT characters into a format understood by the remote system.
- Then receives characters from a pseudo-terminal driver and passes them to the appropriate application.



Network Virtual Terminal(NVT)

NVT is a virtual terminal in TELNET that has a fundamental structure that is shared by many different types of real terminals. NVT (Network Virtual Terminal) was created to make communication viable between different types of terminals with different operating systems.



How TELNET Works?

- **Client-Server Interaction**

The Telnet client initiates the connection by sending requests to the Telnet server.
Once the connection is established, the client can send commands to the server.
The server processes these commands and responds accordingly.

- **Character Flow**
  - When the user types on the local computer, the local operating system accepts the characters.
  - The Telnet client transforms these characters into a universal character set called Network Virtual Terminal (NVT) characters.
  - These NVT characters travel through the Internet to the remote computer via the local TCP/IP protocol stack.
  - The remote Telnet server converts these characters into a format understandable by the remote computer.
  - The remote operating system receives the characters from a pseudo-terminal driver and passes them to the appropriate application program.

Network Virtual Terminal (NVT)

- NVT is a virtual terminal in Telnet that provides a common structure shared by different types of real terminals.
- It ensures communication compatibility between various terminals with different operating systems.

TELNET Commands

Commands of Telnet are identified by a prefix character, Interpret As Command (IAC) with code 255. IAC is followed by command and option codes. The basic format of the command is as shown in the following figure :

TELNET Command Format
Following are some of the important TELNET commands:

Character	Decimal	Binary	Meaning
WILL	251	11111011	1. Offering to enable. 2. Accepting a request to enable.
WON’T	252	11111100	1. Rejecting a request to enable. 2. Offering to disable. 3. Accepting a request to disable.
DO	253	11111101`	1. Approving a request to enable. 2. Requesting to enable.
DON’T	254	11111110	1. Disapproving a request to enable. 2. Approving an offer to disable. 3. Requesting to disable.

Following are some common options used with the telnet:

Code	Option	Meaning
0	Binary	It interprets as 8-bit binary transmission.
1	Echo	It will echo the data that is received on one side to the other side.
3	Suppress go ahead	It will suppress go ahead signal after data.
5	Status	It will request the status of TELNET.
6	Timing mark	It defines the timing marks.
8	Line width	It specifies the line width.
9	Page size	It specifies the number of lines on a page.
24	Terminal type	It set the terminal type.

Code	Option	Meaning
32	Terminal speed	It set the terminal speed.
34	Line mode	It will change to the line mode.

Construction

Selection of devices:

Three Routers: For connecting subnets and ensuring communication between them.

Three Switches: To link multiple PCs within each subnet.

Nine PCs: Representing the end devices that can communicate locally and across subnets.

Cisco Packet Tracer: Used to simulate the network configuration and test its functionality.

Arrangement of Devices and Connection:

Routers:

- **Router 0:** Manages Subnet 1 (192.168.1.0/24) and connects to Switch 0.
- **Router 1:** Acts as the central hub, connecting Subnet 2 (192.168.2.0/24) and providing links to Router 0 and Router 2.
- **Router 2:** Manages Subnet 3 (192.168.3.0/24) and connects to Switch 2.

Switches:

- **Switch 0:** Connects Router 0 to three PCs in Subnet 1.
- **Switch 1:** Connects Router 1 to three PCs in Subnet 2.
- **Switch 2:** Connects Router 2 to three PCs in Subnet 3.

PCs:

Subnet 1 (192.168.1.0/24):

- PC 1: 192.168.1.2
- PC 2: 192.168.1.3

- PC 3: 192.168.1.4

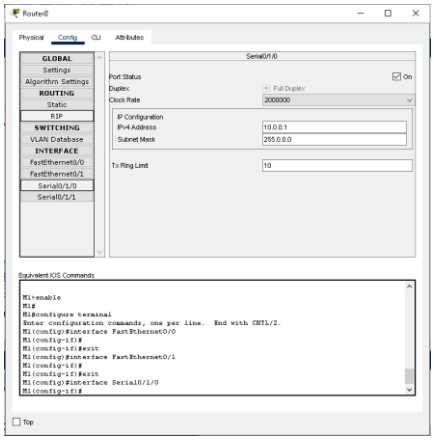
Subnet 2 (192.168.2.0/24):

- PC 4: 192.168.2.2
- PC 5: 192.168.2.3
- PC 6: 192.168.2.4

Subnet 3 (192.168.3.0/24):

- PC 7: 192.168.3.2
- PC 8: 192.168.3.3
- PC 9: 192.168.3.4

Connections



Router-to-Router Connections:

- Router 0 to Router 1: Serial interface (10.0.0.0/30)
- Router 1 to Router 2: Serial interface (20.0.0.0/30)

Router-to-Switch Connections:

- Router 0 to Switch 0
- Router 1 to Switch 1
- Router 2 to Switch 2

Switch-to-PC Connections:

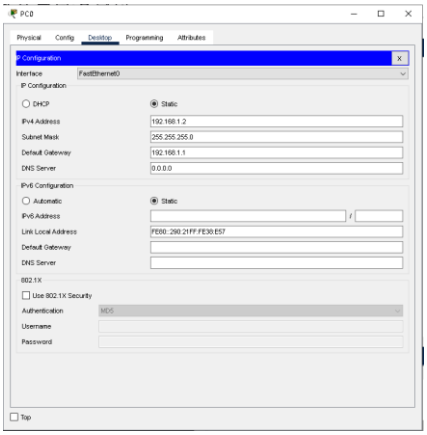
- Each switch connects to three PCs in its respective subnet.

Connection Media

- **Serial Cables:** Used for connecting routers.
- **Ethernet Cables:** Used for connecting routers to switches and switches to PCs.

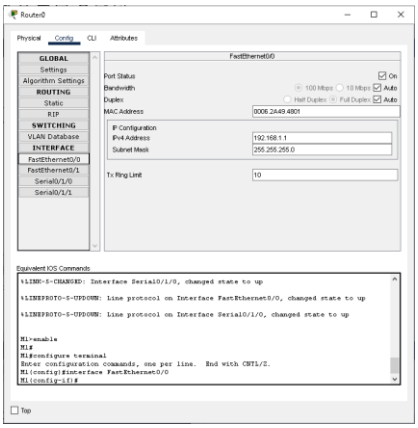
Configuration Step

Step 1: Configure Routers



Assign IP Addresses to Router Interfaces:

- Click on the router0
- go to the config tab
- access the gigabit ethernet0/0
- turn on the services
- Put the following details:
    - IP Address: 192.168.1.1
    - Subnet mark: 255.255.255.0

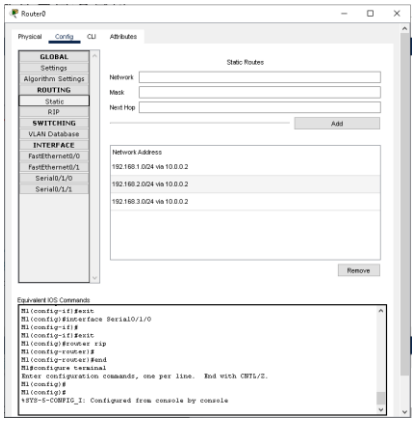


Configure Serial Interfaces:

- Click on the router0
- Go to config>serial0/0/0
- Tern oh the services
- Put the following details:
    - IP Address: 10.0.0.1
    - Subnet mark: 255.0.0.0

Enable Routing:

- Click on the Router0
- Go to config>static
- Put the following details:
    - Network: 192.168.1.0
    - Mask: 255.255.255.0
    - Next Hop: 10.0.0.2

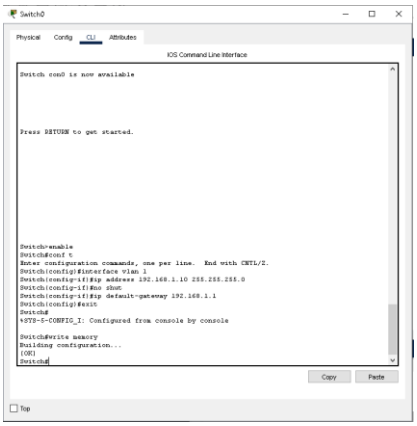


(Repeat the same configuration on Router1 and Router2 according to their subnet and IP addressing and serial interface)

Step 2: Configure Switches

- Basic IP Configuration:

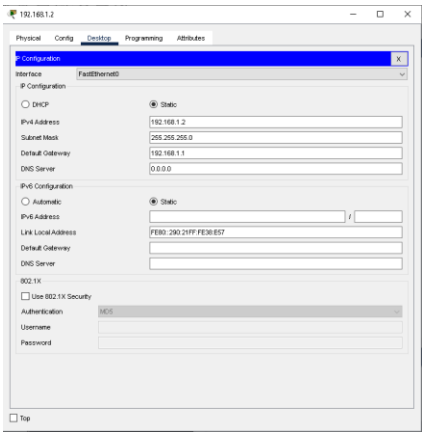
- Access the CLI of each switch and configure basic settings.
- Switch> enable
- Switch# configure terminal
- Switch(config)# hostname S0
- S0(config)# interface vlan 1
- S0(config)#ip addressing 192.168.1.10 255.255.255.0
- S0(config)#no shutdown
- S0(config)#exit
- S0#write memory



<u>Step 3:</u> Configure PCs

Assign Static IP Addresses:

On each PC, configure the IP address, subnet mask, and default gateway according to corresponding subnet.



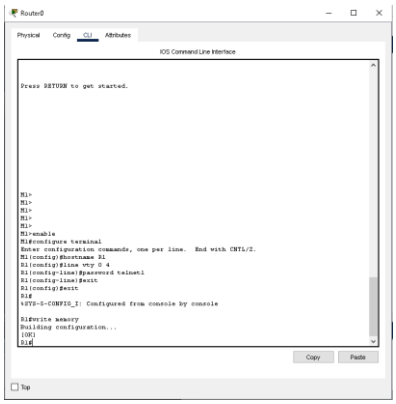
- Go to desktop>IP cong.
- Put the following:
    - IP Address: 192.168.1.2
    - Subnet Mask: 255.255.255.0
    - Default Gateway: 192.168.1.1

Test Connectivity:

Use the ping command to verify that the PCs can communicate with their gateway.

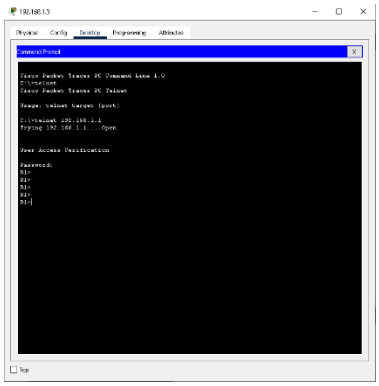
<u>Step 4:</u> Configure Telnet on Routers

Enable Telnet Access:



- **On each router, enable Telnet by setting up a VTY password.**
    - Router(config)#hostname R0
    - R0(config)# line vty 0 4
    - R0(config-line)# password telnet123
    - R0(config-line)# login
    - R0(config-line)# exit
    - R0(config)#exit
    - R0#write memory

<u>Step 5:</u> Test Network Connectivity



Ping Across Subnets:

- Test connectivity between PCs in different subnets using the ping command.

Test Telnet Access:

- From a PC, access a router using Telnet.
    - telnet 192.168.1.1
- Enter the configured Telnet password to access the router's CLI.

Network and Analysis

Network Performance Evaluation

Network performance is vital for efficiency and functionality. Key evaluation factors include:

1. **Latency and Response Time**: Tested using the ping command, minimal delays were observed, indicating optimized routing and physical connections.
2. **Throughput**: Sufficient bandwidth for subnet intercommunication and Telnet sessions was confirmed, with stable throughput supported by Ethernet connections.
3. **Connectivity**: Devices communicated within and between subnets, verifying proper routing and IP assignments. Remote Telnet sessions were successful, confirming access configuration.
4. **Reliability**: Failover tests showed the network's stability during device shutdowns, demonstrating robustness without disruptions.

Achievements

- **Telnet Access**:
Telnet was implemented on routers for remote access, with secure authentication measures.
- **Effect on Routing**:
Static routing was correctly configured, ensuring smooth communication between subnets without routing loops or misconfigurations.
- **Device Integration**:
Routers, switches, and PCs worked seamlessly, with LANs and subnetting dividing network traffic logically.
- **Security Improvement**:
Security measures included password protection, access control lists, and secure protocols to protect the network.
- **Testing**:
Extensive testing confirmed the network's reliable performance, with proper connectivity and remote access functionality.

Problems

Some problems which occur during configuration of Telnet are as following;

- **Misconfigurations**: IP and routing errors caused connectivity issues.
- **Telnet Security**: Lack of encryption addressed with strong passwords and restrictions.
- **Cable Management**: Physical connections needed careful organization to avoid issues.
- **Troubleshooting**: Significant time spent resolving network issues in testing.
- **Scalability**: Future expansion may require routing redesign and hardware upgrades.

Uses of TELNET

Some main uses of Telnet are as following;

- Remote Administration and Management
- Network Diagnostics
- Understanding command line interface.
- Accessing Bulletin Board Systems (BBS)
- Automation and Scripting

Advantages of TELNET

Some main advantages of using Telnet are as following;

- It provides remote access to someone’s computer system.
- Telnet allows the user for more access with fewer problems in data transmission.
- Telnet saves a lot of time.
- The oldest system can be connected to a newer system with telnet having different operating systems.

Disadvantages of TELNET

Some main disadvantages of using Telnet are as following;

- As it is somehow complex, it becomes difficult to beginners in understanding.
- Data is sent here in form of plain text, that's why it is not so secured.
- Some capabilities are disabled because of not proper interlinking of the remote and local devices.

Tools and Resources

Tools used:

- **Packet Tracer/ GNS3**: Network simulators to test and visualize network configurations.

Resources for Further Reading:

- "Data communication and Networking" by **BEHROUZ A. FOROUZAN.**
- Introduction to TELNET - GeeksforGeeks
- What is Network Virtual Terminal in TELNET? - GeeksforGeeks

Learning Outcomes

- **Network Design and Topology**: Gained insights into designing efficient networks with routers, switches, and subnetting.
- **Routing Configuration**: Learned static routing and the importance of accurate routing tables for inter-subnet communication.
- **Remote Access Management**: Configured Telnet for remote access, understanding its security limitations and SSH advantages.
- **Troubleshooting Skills**: Used tools like ping and traceroute for problem-solving.
- **Security Awareness**: Learned to secure networks with passwords, access control lists, and encryption.
- **Teamwork and Planning**: Emphasized effective collaboration and documentation.

Conclusion

Summary of the Project

This project aimed to design and configure a network to demonstrate the functionality of remote access using Telnet. The network comprised three routers, three switches, and nine computers, interconnected to form a robust topology that supported communication between subnets.

Key configurations included:

1. Assigning static IP addresses to routers, switches, and PCs.
2. Configuring routing to enable inter-subnet communication.
3. Establishing Telnet access for remote management of routers.
4. Implementing security measures to safeguard network resources.

The project successfully achieved its objectives by:

- Enabling seamless communication between all devices.
- Demonstrating secure and functional Telnet-based remote access.
- Ensuring network stability and performance through rigorous testing.ss