Telnet Cheat Sheet

A quick reference guide to using Telnet, covering basic commands, connection management, and security considerations. This cheat sheet provides a concise overview for network troubleshooting and remote access tasks.

Basic Telnet Commands

Connecting to a Host

`telnet <hostname>`	Connect to the specified hostname using the default Telnet port (23). **Example:** `telnet example.com`
`telnet <hostname> <port>`	Connect to the specified hostname on a specific port. **Example:** `telnet example.com 80` (Connect to port 80)
`open <hostname> <port>`	Opens a connection to the specified hostname and port from within the Telnet client. **Example:** `open example.com 25` (Connect to port 25)

Telnet Client Commands

`close`	Closes the current connection.
`quit` or `exit`	Closes the current connection and exits the Telnet client.
`status`	Displays the current status of the Telnet client, including connection information.
`display`	Displays the Telnet client settings.
`?` or `help`	Displays a list of available Telnet commands.

Sending Special Characters

`send <command>`	Sends special Telnet commands to the server. Common commands include: `ao` (Abort Output), `ayt` (Are You There), `esc` (Escape), `ip` (Interrupt Process), `nop` (No Operation), `synch` (Synchronize).
`send ao`	Aborts the output on the remote system.
`send ip`	Interrupts the current process on the remote system.

Advanced Telnet Usage

Negotiation Options

`set <option> <value>`	Sets various Telnet options. Common options include `echo` (local echoing), `crmod` (carriage return mode), and `termtype` (terminal type). **Example:** `set echo on` (Enable local echoing)
`unset <option>`	Unsets a previously set Telnet option. **Example:** `unset echo` (Disable local echoing)
`toggle <option>`	Toggles a boolean Telnet option between on and off. **Example:** `toggle crlf` (Toggle carriage return/line feed mode)

Local Echo and Line Mode

`set echo`	Enables local echoing, so characters typed are displayed on your screen.
`unset echo`	Disables local echoing; useful if the server is already echoing characters.
`set crlf`	Sends carriage return and line feed characters. Some servers may require this.
`unset crlf`	Sends only carriage return characters.

Terminal Emulation

`set termtype <type>`	Sets the terminal type to a specific value (e.g., `vt100`, `ansi`). Some servers adapt their output based on terminal type. **Example:** `set termtype vt100`
`display termtype`	Displays the currently set terminal type.

Troubleshooting and Security

Common Issues

If you cannot connect, verify the hostname or IP address and port number are correct.

Check if a firewall is blocking the connection on port 23 (or the specified port).

If you see garbled output, try setting the terminal type (`set termtype`) to a common value like `vt100` or `ansi`.

If characters are not displaying correctly, ensure local echoing is enabled or disabled as needed (`set echo` or `unset echo`).

Security Considerations

Warning: Telnet transmits data in plaintext, including usernames and passwords. This makes it vulnerable to eavesdropping and should generally be avoided on untrusted networks.

Consider using SSH (Secure Shell) instead, which encrypts all transmitted data.

If you must use Telnet, avoid transmitting sensitive information and only connect to trusted servers.

Never use Telnet over public Wi-Fi or other untrusted networks.

Alternatives to Telnet

SSH (Secure Shell) is the preferred alternative for secure remote access. It encrypts all transmitted data, protecting against eavesdropping.

Command: `ssh <username>@<hostname>`

For remote desktop access, consider using protocols like RDP (Remote Desktop Protocol) or VNC (Virtual Network Computing), which offer graphical interfaces and often support encryption.

Practical Telnet Examples

Connecting to an SMTP Server

`telnet mail.example.com 25`	Connects to the SMTP server on `mail.example.com` on port 25. You can then issue SMTP commands to test mail server functionality.
`HELO example.com`	Initiates an SMTP HELO handshake. Replace `example.com` with your domain.
`QUIT`	Closes the SMTP connection.

Connecting to a Web Server

`telnet example.com 80`	Connects to the web server on `example.com` on port 80. You can then send HTTP requests.
`GET / HTTP/1.0`	Sends a simple HTTP GET request for the root page. Press Enter twice after this line.
Press Enter Twice	After the `GET` command, you must press Enter twice to send the request.

Port Scanning with Telnet

Telnet can be used to quickly check if a port is open on a remote host.

Try connecting to various ports using `telnet <hostname> <port>`. If the connection succeeds, the port is likely open. If the connection fails or times out, the port is likely closed or filtered.

This is a rudimentary form of port scanning and should be used cautiously, respecting network policies and avoiding unauthorized scanning.