Dropbear

We use dropbear, which is a lightweight ssh server, to remotely connect to a device using the ssh protocol in an efficient manner. Dropbear can be used for small binary, ram, which also makes it fast.

In the router terminal: to get into router terminal: ssh username@ipaddress (ssh root@192.168.1.1)

nano /etc/config/dropbear

```
config dropbear
        option PasswordAuth 'on'
        option RootPasswordAuth 'on'
        option Port '22'
        option Interface ‘lan’
        option enable ‘1’
```

This is the dropbear configuration that we can customize to enable or disable a connection via ssh.
1. PasswordAuth: If it's 'off', and you haven't set up public/private SSH keys, you'll get a "Permission denied" message.
2. RootPasswordAuth: if ‘off’, on root users, does not allow password login, we should use the ssh key to connect to the device, on non-root users, connection is refused.
3. Port: by default the port number for ssh is ‘22’. If changed, connection will be refused.
4. Interface: specifies the types of interfaces that can connect via ssh. If it is set to wan, and we use a lan interface, connection will be refused.
5. enable: set to ‘1’ means enabled, ‘0’ means it is disabled. If ‘0’ the connection will be refused.

Thus we can use dropbear to customize the configuration, and allow connections via ssh protocol.

Any changes made will take effect only after restarting the dropbear:
/etc/init.d/dropbear restart

Unified Configuration Interface(UCI): it has all the configuration files like dropbear, network, etc…., which can be used to customize configuration as per requirement.
We can even set a particular configuration file, by using the command, uci set - - - -.