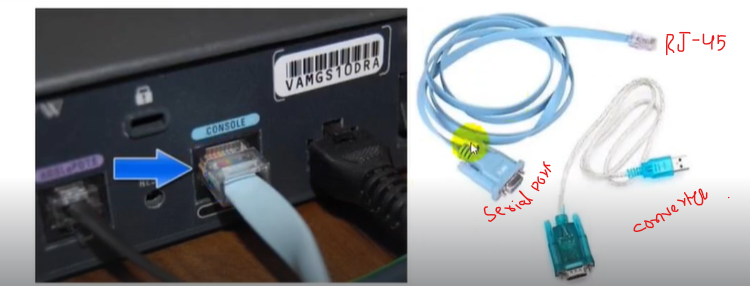
Cisco management devices, Console Telnet, SSH

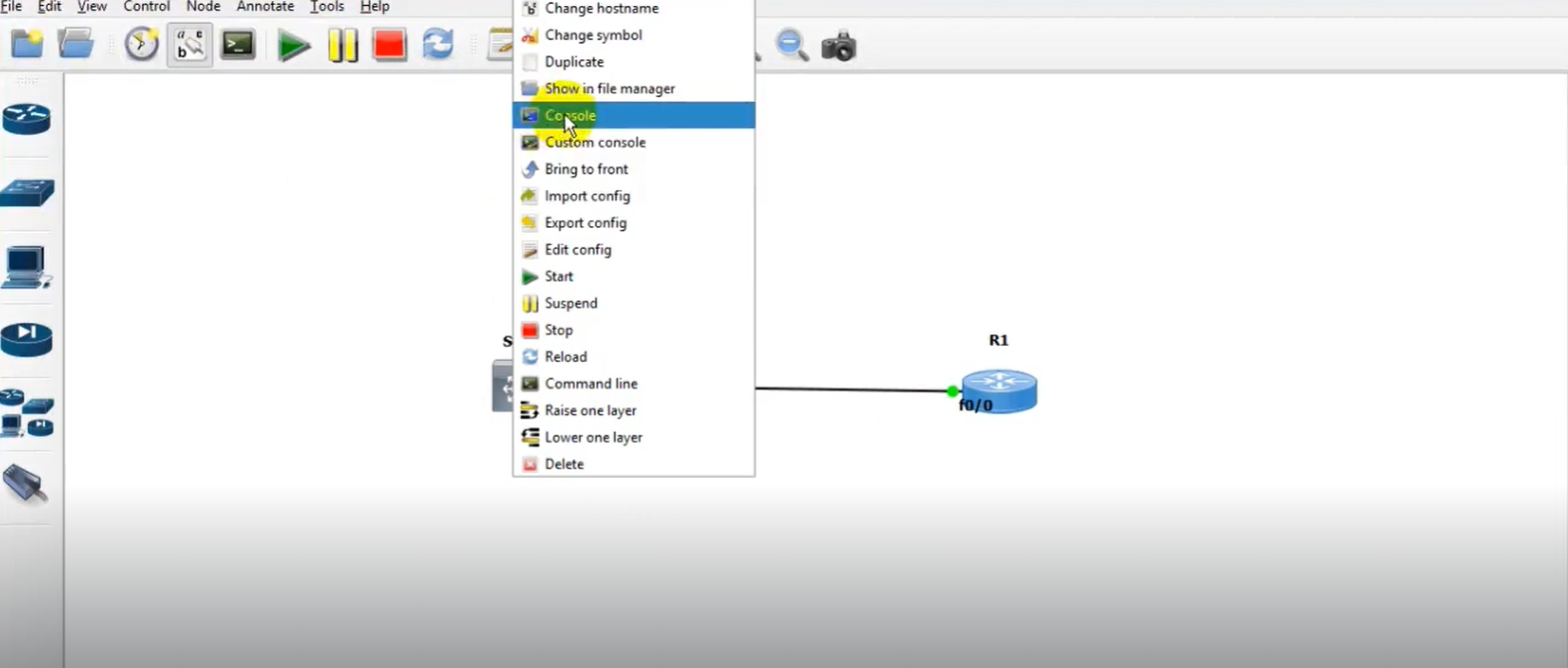
**Device Management**

* Traffic that network administrator uses to configure network devices is Management.
* Management plane traffic is usually consisting protocol traffic like Telnet, SSH or SNMP.
* Management plane provides the ability to manage network infrastructure devices.
* First step toward management is to set username and password.

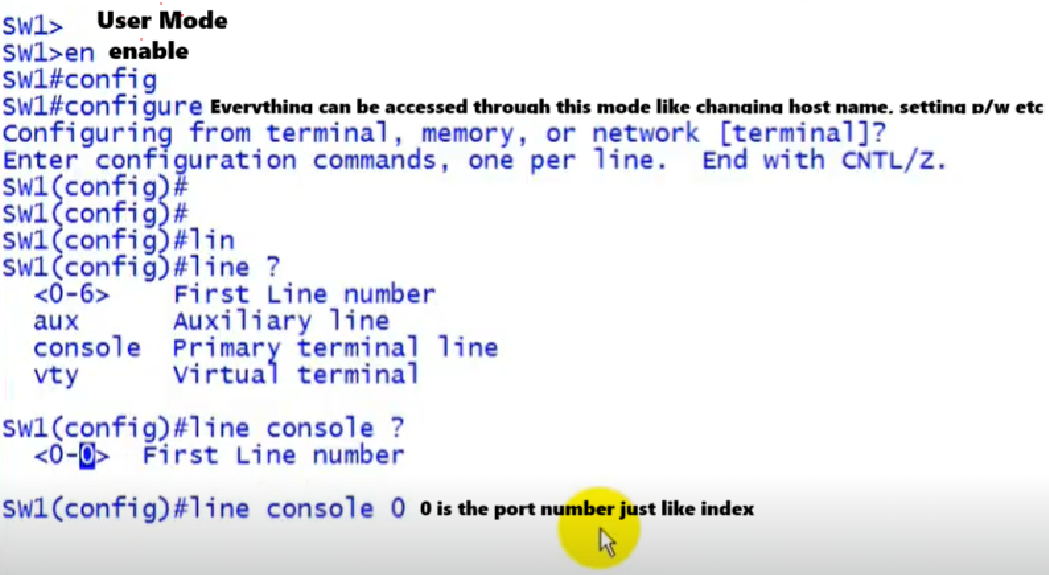
**Console Port**

* Every Cisco Router, Firewall or a Switch has a console port.
* Console port also known as the management port on its backside.
* Console port is used to connect a computer directly to a router or switch.
* It manages the router or switch since there is no display device for a router or switch.
* The console port must be used to initially to install routers.
* There is no network connection initially to connect using SSH, HTTP or HTTPS.
* Normally router, switch or firewall console port is a RJ45 port.
* Console port is the management port, which is used by administrators.



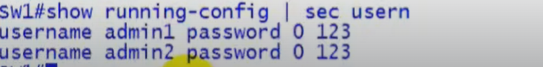
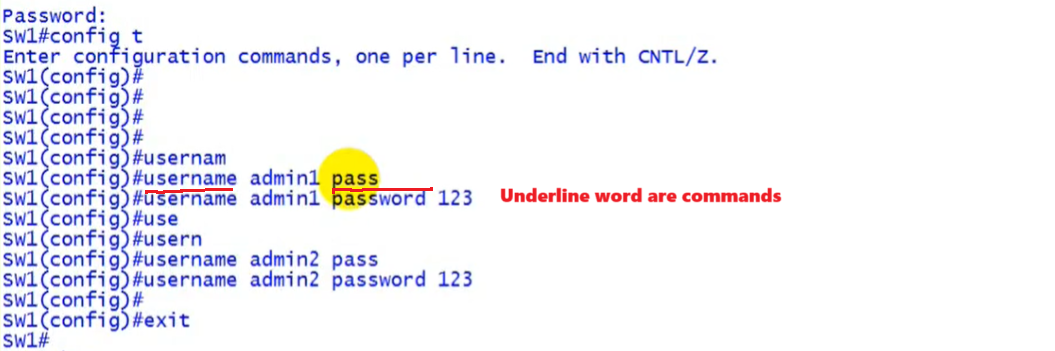


* This will allow us to work virtually on console of switch for practice.

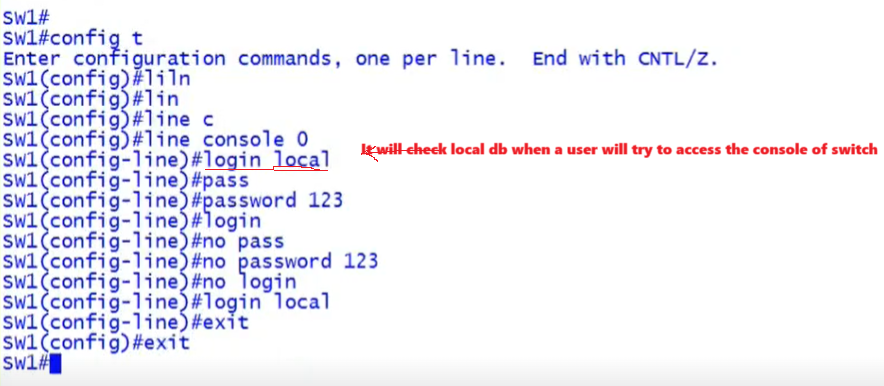


* After just setting p/w then setting username and p/w to secure console.

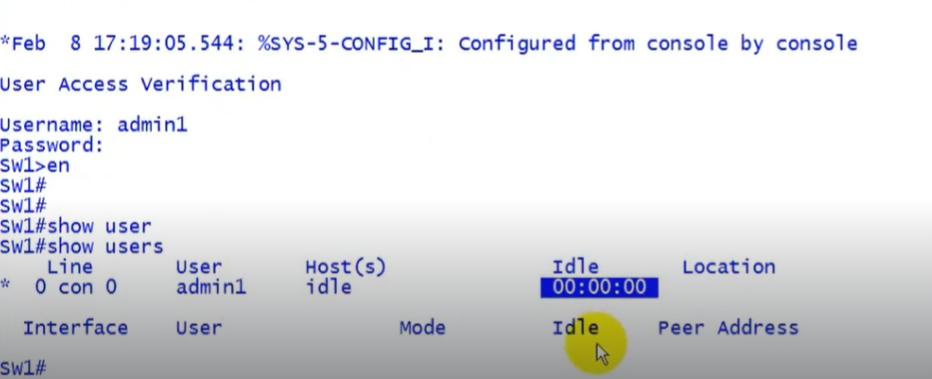
**Setting up Username And P/W**



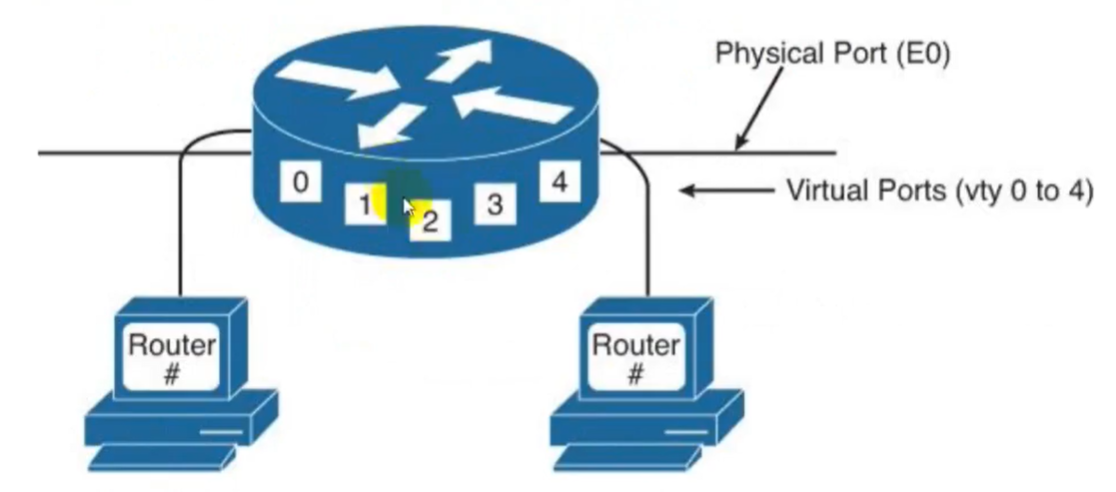
* Now these are in local data base so in configuration mode it must be specified **login local**.



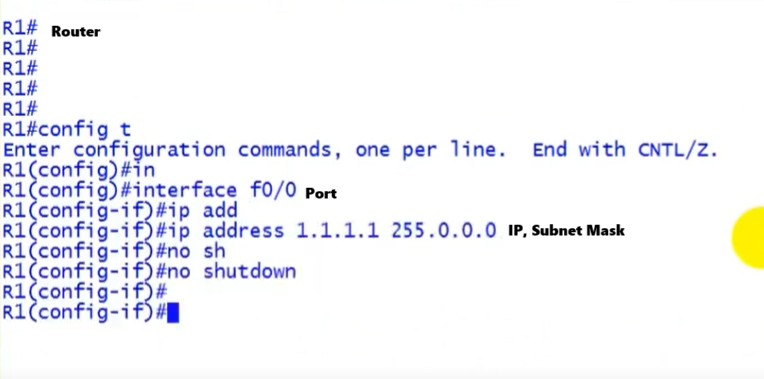
**Log in User Detail:**

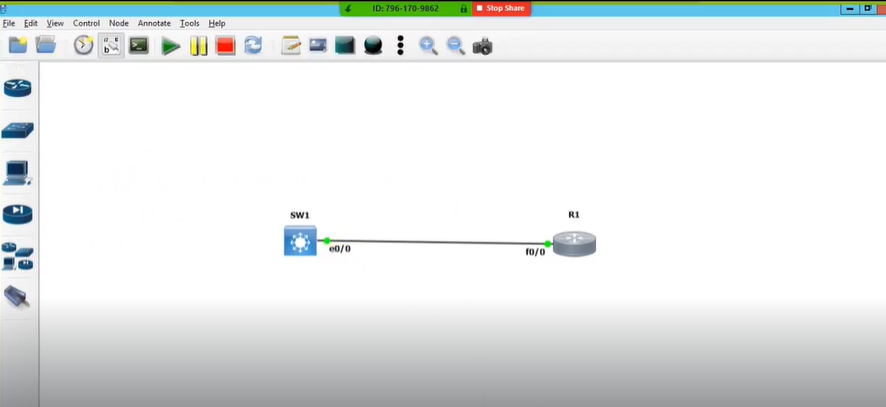
****

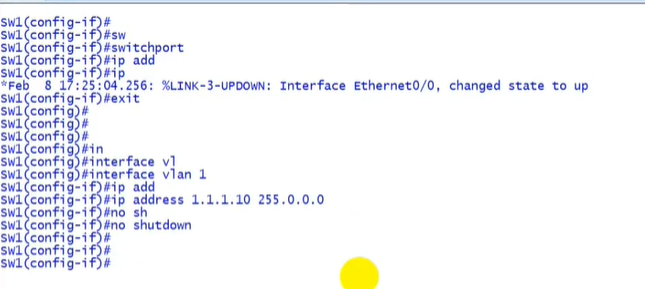
**VTY (Virtual Terminal Lines):**

* VTY stands for Virtual Terminal Lines or Virtual Teletype.
* VTY is a Command Line Interface (CLI) created in a router.
* VTY is used to facilitate a connection to the daemon via Telnet.
* VTY is just a way of accessing the switches or routers CLI remotely.
* Virtual Terminals are logical connections from the network to the router.
* VTY are typically telnet connections to switches or routers.
* Telnet is use to manage routers or switches remotely.
* A Telnet client and server application ships with Cisco's IOS software.
* ****Telnet commonly uses TCP port 23 to connect to devices.

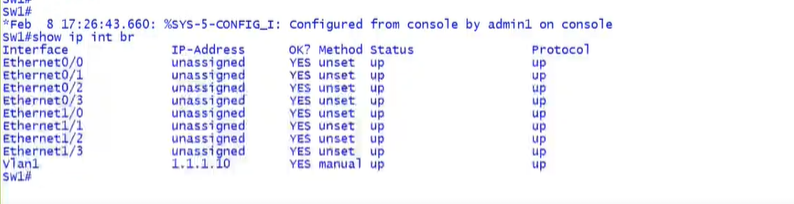
Assigning IP to Router For Telnet(Teletype Network)

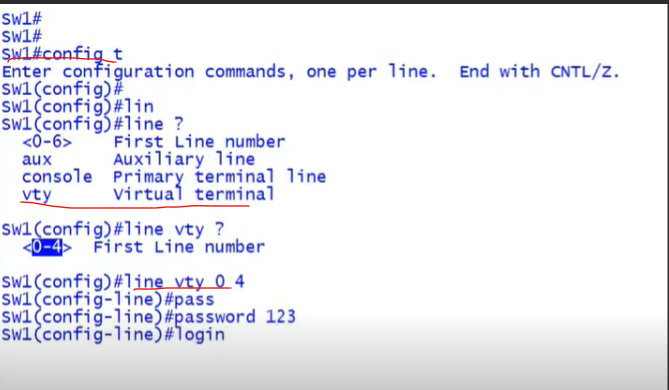




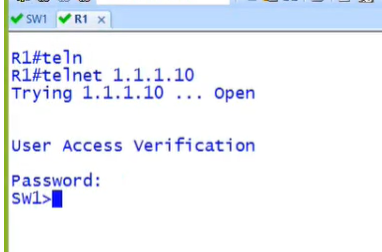
  
**Assiging IP to Switch(Layer 2[no switch])**

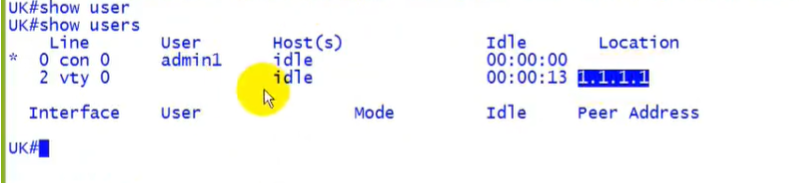
* **SVI (Switch virtual Interface)** allows to assign IP in Layer 2 Switch for Telnet

**Show IP For Telnet:**

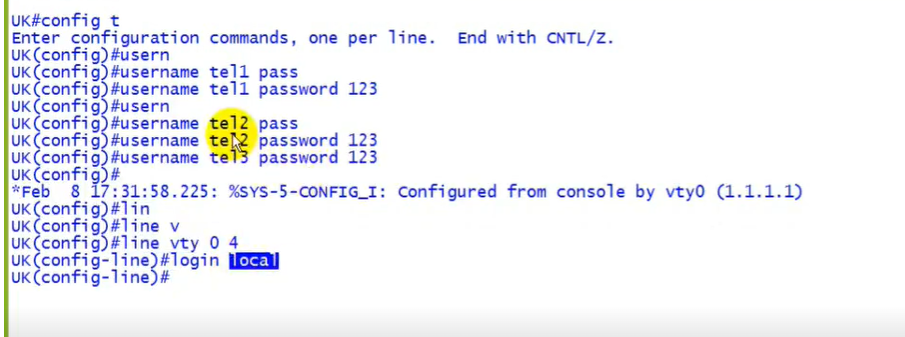
****

**TELNET:**

* It allows us to remotely control switch means the router or any device connected to switch using the terminal of that device we can configure Switch.
* In this picture we used router terminal to access switch Router is also connected to switch.

**Check Accessed User of Switch:** 

**Set Username & P/W for TELNET:**

****

**SSH (Secure Shell):**

* SSH stands for Secure Shell.
* SSH provides a secure remote access connection to network devices.
* SSH are two versions SSH Version I and SSH Version 2.
* Communication between the client & server is encrypted in both SSH version.
* SSH, version 2 is more secure than version SSH Version 1.
* SSH commonly uses TCP port 22 to connect to devices.
* SSH, as the preferred management protocol under the VTY interfaces.
* SSH provides a secure and reliable mean of connecting to remote devices.
* SSH, Version 2 is the more secure and commonly used version.
* SSH, require an IOS image that supports crypto features.
* SSH is a more secure way to configure routers, switches or firewalls.
* SSH requires a RSA public and private Key pair.
* Router & Switch Name should be different like sw (no). additinaly domain is required to generate key.