Device Management:

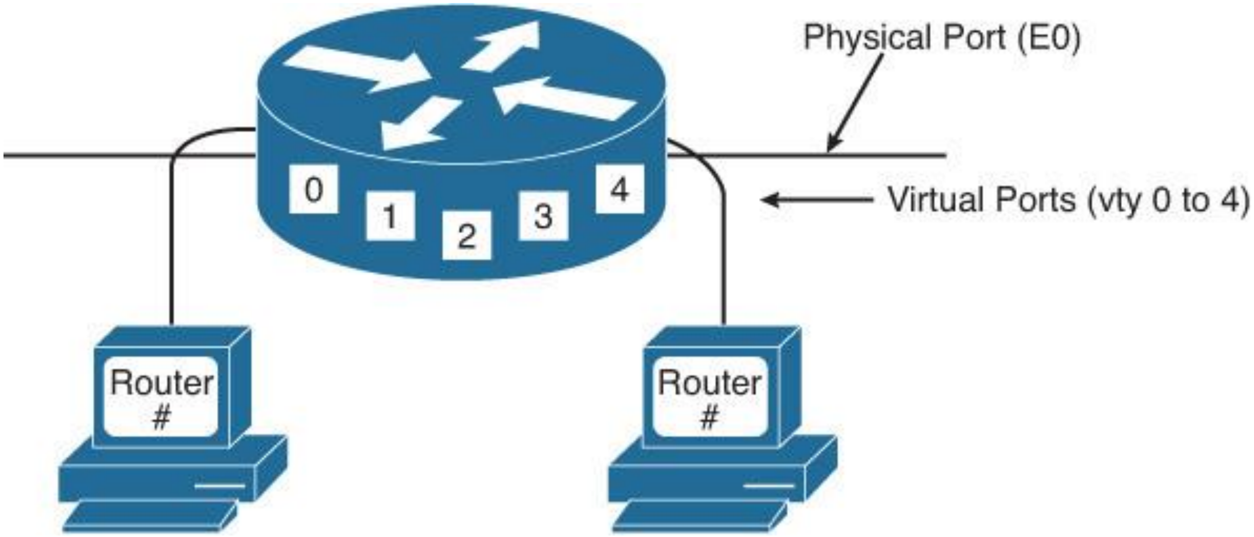
- Traffic that network administrator uses to configure network devices is Management.
- Management plane traffic is usually consists protocol traffic like Telnet, SSH or SNMP.
- Management plane provides the ability to manage network infrastructure devices.
- First step toward management is to set username 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 manage 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.
- Console port can be used to log into a router directly without network connection.
- Console require a terminal emulator application like PuTTY to connect to router.
- Console port connect to router when a router cannot be accessed over the network.

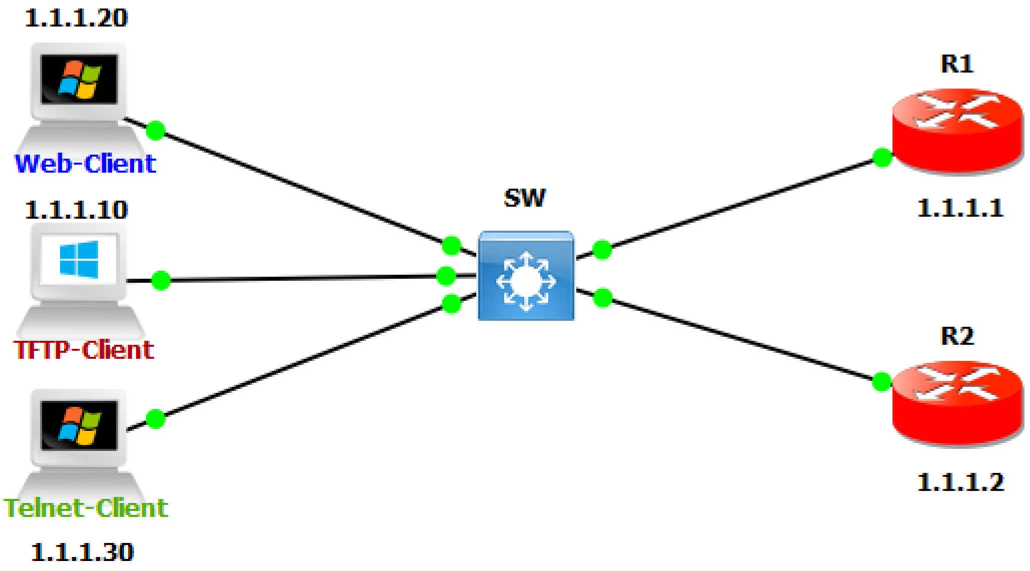
VTY (Virtual Terminal Lines):

- 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.



SSH (Secure Shell):

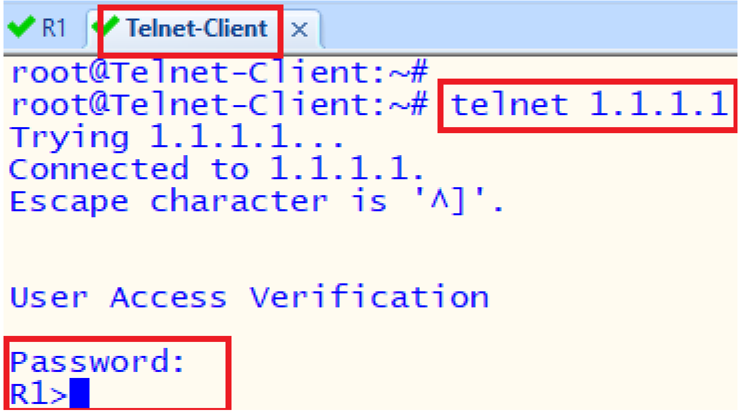
- SSH stands for Secure Shell.
- SSH provides a secure remote access connection to network devices.
- SSH are two versions SSH Version 1 and SSH Version 2.
- Communication between the client & server is encrypted in both SSH version.
- SSH, version 2 is more secure than version SSH Version 1.
- SSH commonly 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.



Configure Console Authentication Router	
Password Only	**Username & Password**
R1(config-)≠ line console 0 R1(config-line)≠ password cisco R1(config-line)≠ login	R1(config-)≠ username admin password cisco R1(config-)≠ line console 0 R1(config-line)≠ login local
AAA Local Database	
R1(config)# aaa new-model R1(config)# aaa authentication login default local R1(config)≠ username admin password 123 R1(config)# line console 0 R1(config-line)# login authentication default	

Configure VTY Authentication Router	
Password Only	**Username & Password**
R1(config-)≠ line vty 0 4 R1(config-line)≠ password cisco R1(config-line)≠ login	R1(config-)≠ username admin password cisco R1(config-)≠ line vty 0 4 R1(config-line)≠ login local
AAA Local Database	
R1(config)# aaa new-model R1(config)# aaa authentication login default local R1(config)≠ username admin password 123 R1(config)# line vty 0 4 R1(config-line)# login authentication default	
R1(config)#access-list 1 permit host 1.1.1.10 R1(config)#line vty 0 4 R1(config-line)#access-class 1 in	

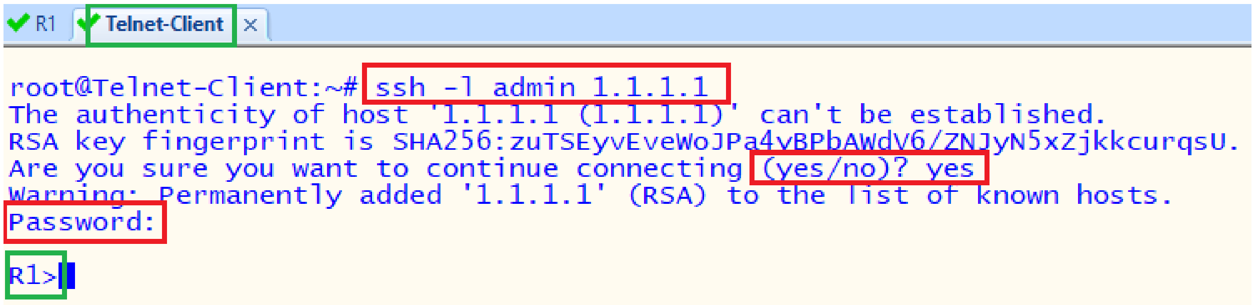
SSH Configurations	
R1(config)# hostname R1	R1(config)# ip domain-name ksa.com
R1(config)# crypto key generate rsa	R1(config)# ip ssh authentication-retries 3
R1(config)# ip ssh timeout 60	R1(config)#ip ssh version 2
R1(config)#username admin password 123	R1(config)#crypto key zeroize rsa
R1(config)#line vty 0 4 R1(config-line)#login local R1(config-line)#transport input ssh	R1#show crypto key mypubkey rsa R1#show ssh R1#show ip ssh
R2#ssh -l admin 1.1.1.1	R1#show users



```
root@Telnet-Client:~#
root@Telnet-Client:~# telnet 1.1.1.1
Trying 1.1.1.1...
Connected to 1.1.1.1.
Escape character is '^]'.


User Access Verification

Password:
R1>
```



```
root@Telnet-Client:~# ssh -l admin 1.1.1.1
The authenticity of host '1.1.1.1 (1.1.1.1)' can't be established.
RSA key fingerprint is SHA256:zuTSEyvEveWoJPa4vBPbAWdV6/ZNJyN5xZjkkcurqsU.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '1.1.1.1' (RSA) to the list of known hosts.
Password:

R1>
```