Lab 3

1. Recreate SSH key by using 2048 bit with SSH v2.0
   1) Previous SSH version

```
!
!
username adminssh password 0 adminssh01
!
!
!
!
!
!
!
ip ssh version 1
ip domain-name netsec.com
!
!
spanning-tree mode pvst
!
!
!
!
```

ip ssh version 1

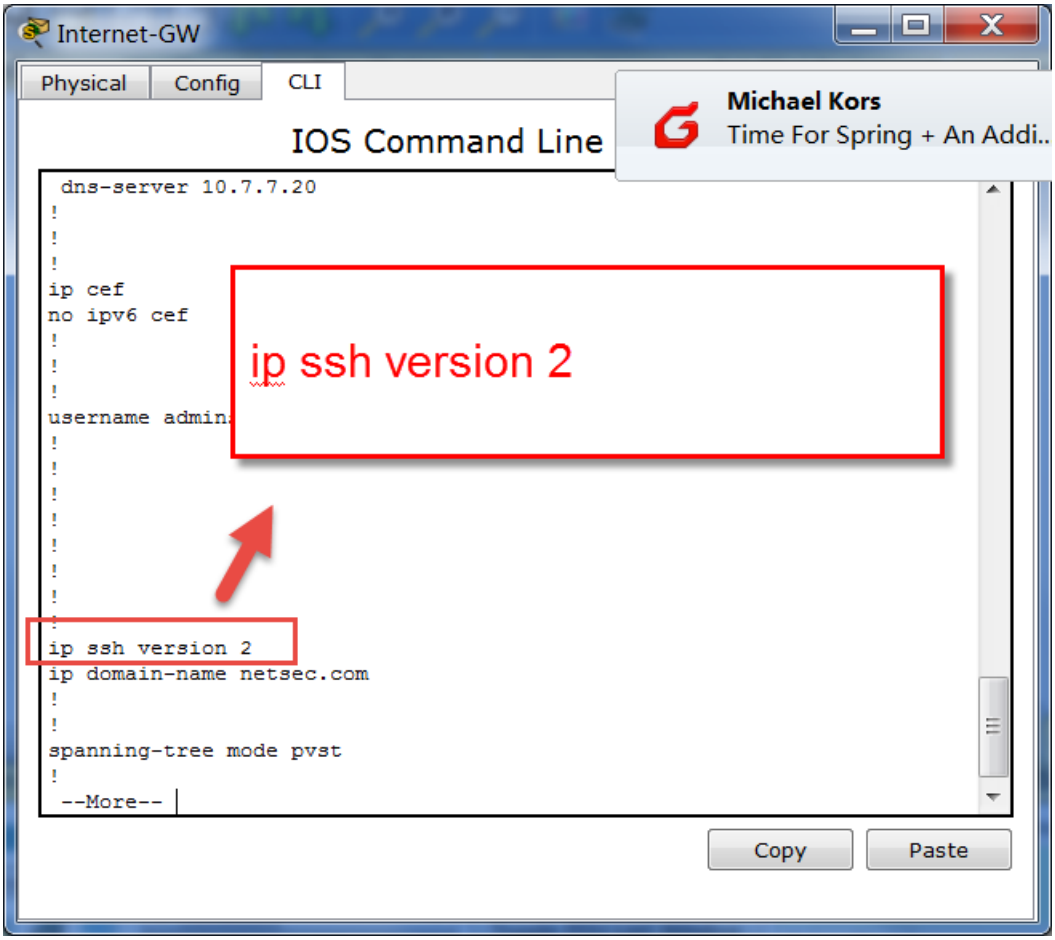
   2) Changing

```
ciscoasa#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ciscoasa(config)#ip ssh version 2
Please create RSA keys (of at least 768 bits size for your reason)
ciscoasa(config)#crypto key generate rsa
% You already have RSA keys defined named ciscoasa.netsec.com
% Do you really want to replace them? [yes/no]: yes
The name for the keys will be: ciscoasa.netsec.com
Choose the size of the key modulus in the range of 512 to 2048 for
  General Purpose Keys. Choosing a key modulus greater than 512 may
  a few minutes.

How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]

ciscoasa(config)#ip ssh version 2
*?? 1 1:5:32.814:  %SSH-5-ENABLED: SSH 1.99 has been enabled
ciscoasa(config)#
```

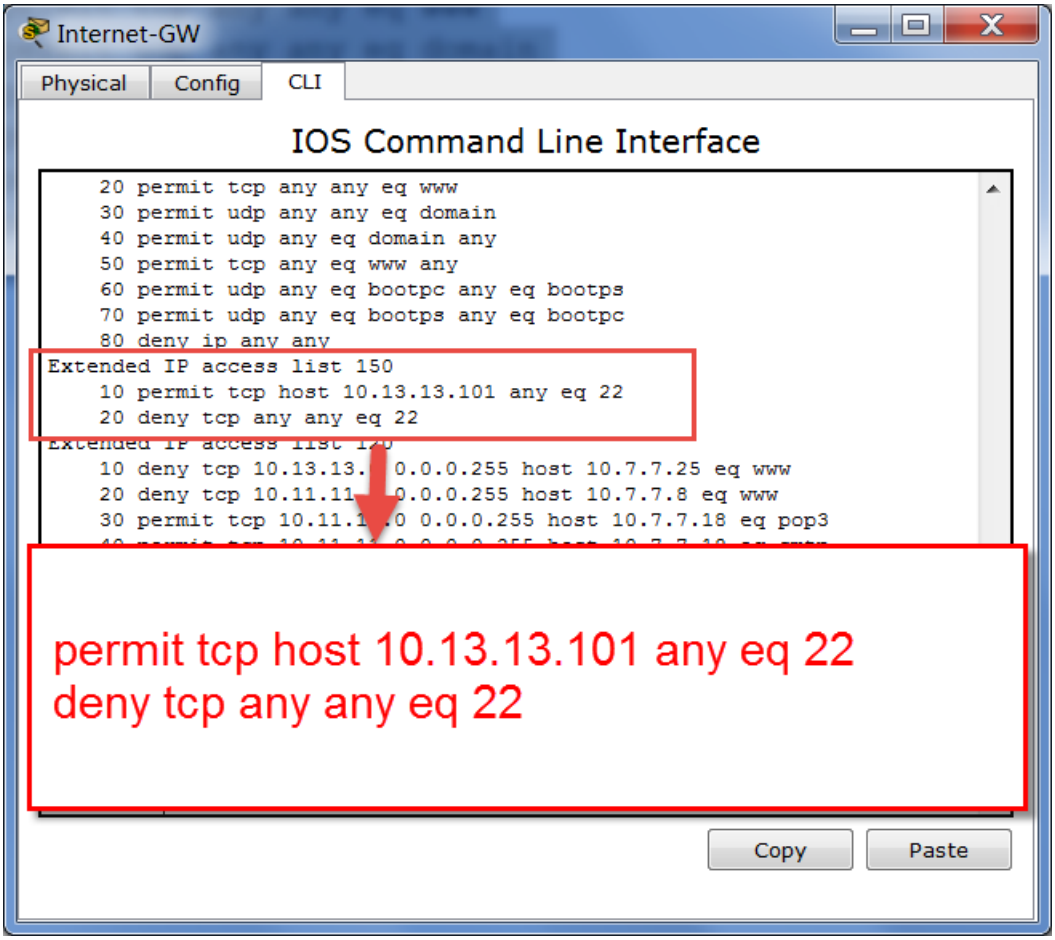
2048

ip ssh version 2

3) Post changing SSH version



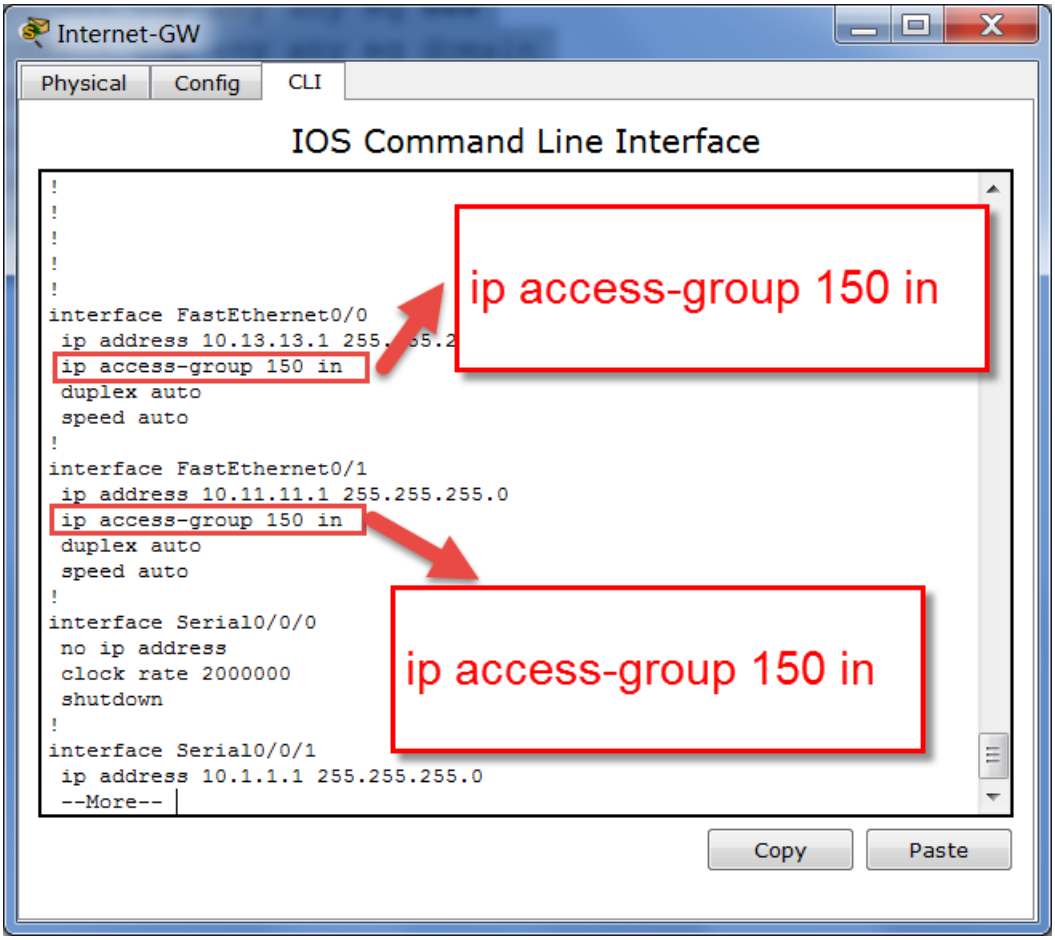
2. Create ACL and limit access to SSH to the Internet-GW router to only Student2-pc and apply it to the correct interfaces to limit access.
   1) Access list



Description:
According to the requirement, only student 2 from engineering college (ip: 10.13.13.101) can SSH Internet/GW router (ip: 10.13.13.1). So, in this case, we set up ACL as above. And, we will default deny any other host to use SSH services. However, if we only want block other SSH to a specific router Internet/GW without block all other SSH connections, we need to change deny entry to

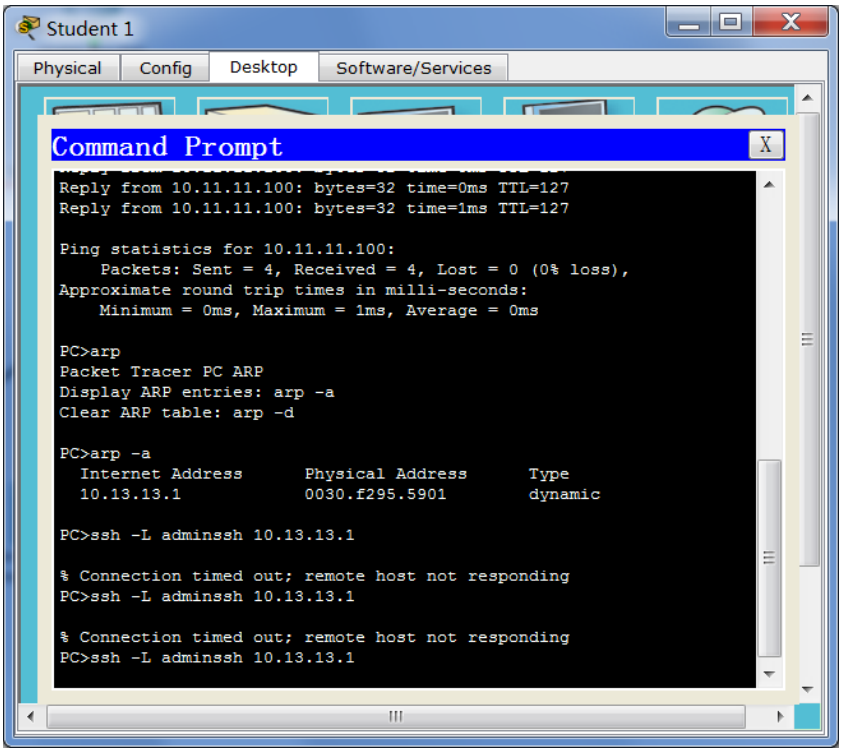
Deny tcp any 10.13.13.1 eq 22

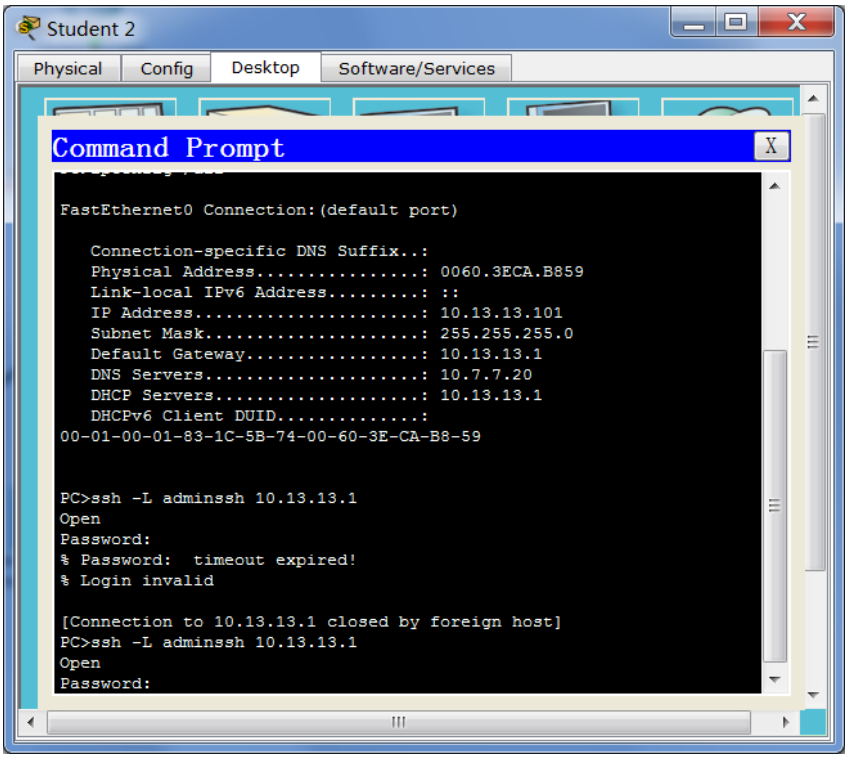
2) Interface apply

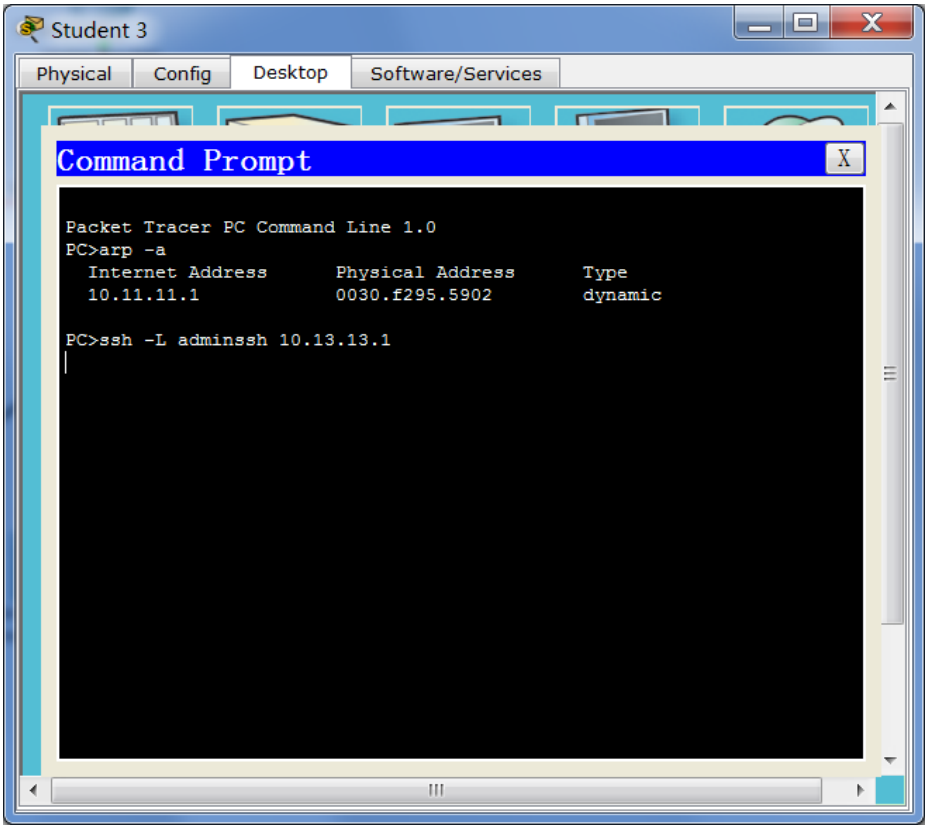


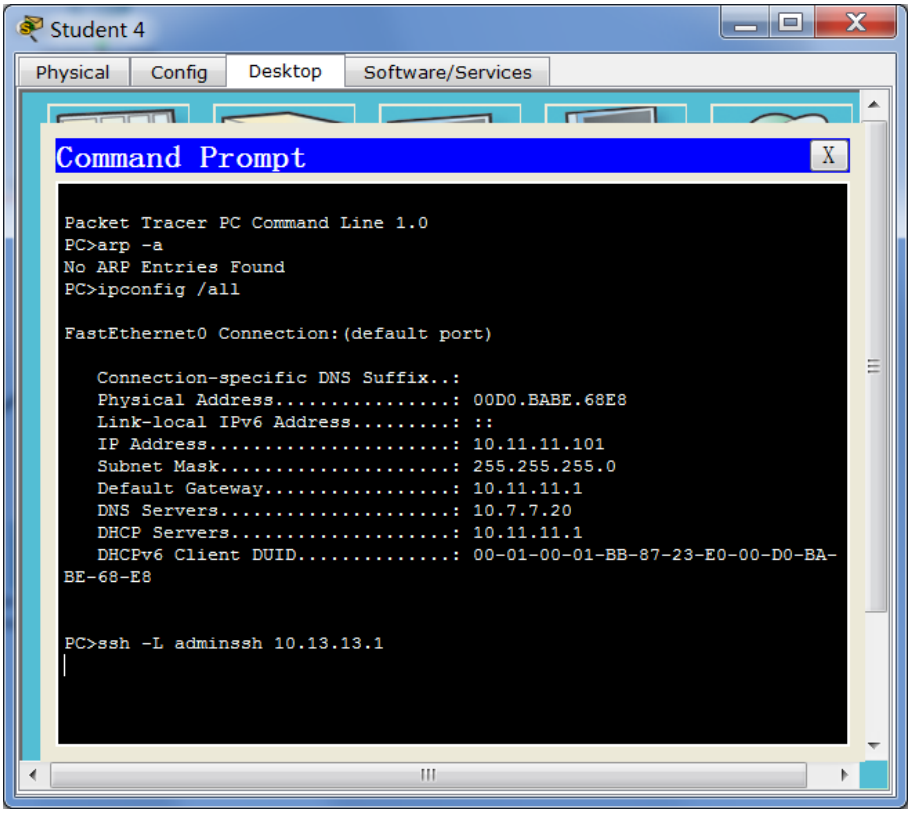
In this case, we applied to two interface: Fastethernet 0/0 and fastethernet 0/1. The reason is we need to block both Engineering Department and CCIS Department from sshing the Internet/GW router.

3) Verification





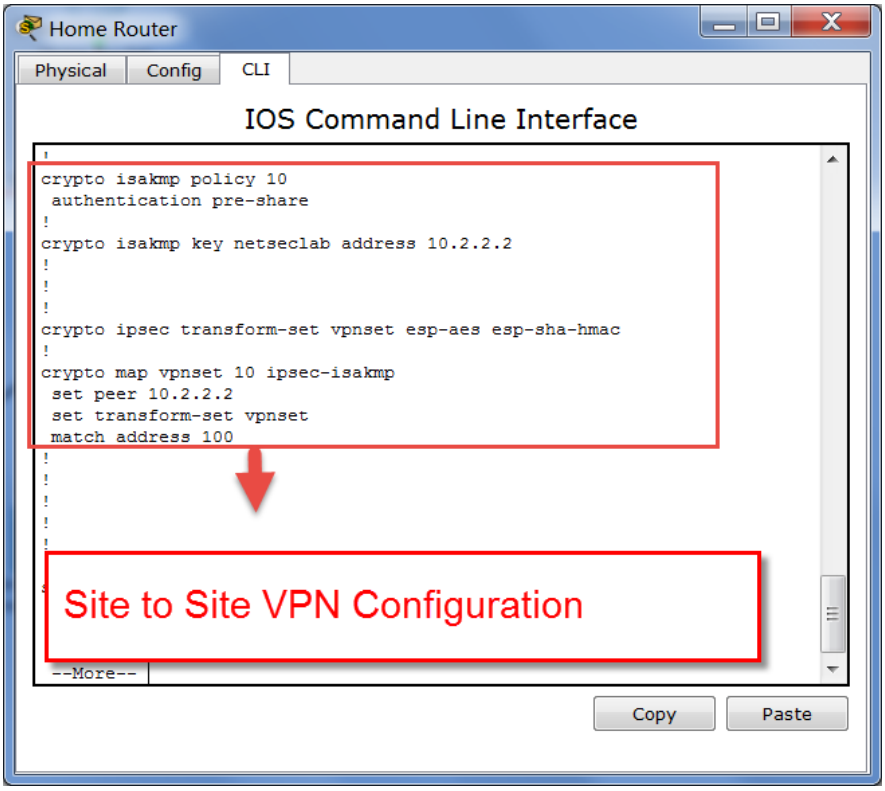




Only student 2 can SSH.

3. Site-To-Site VPN settings.

1) VPN configuration



2) Results