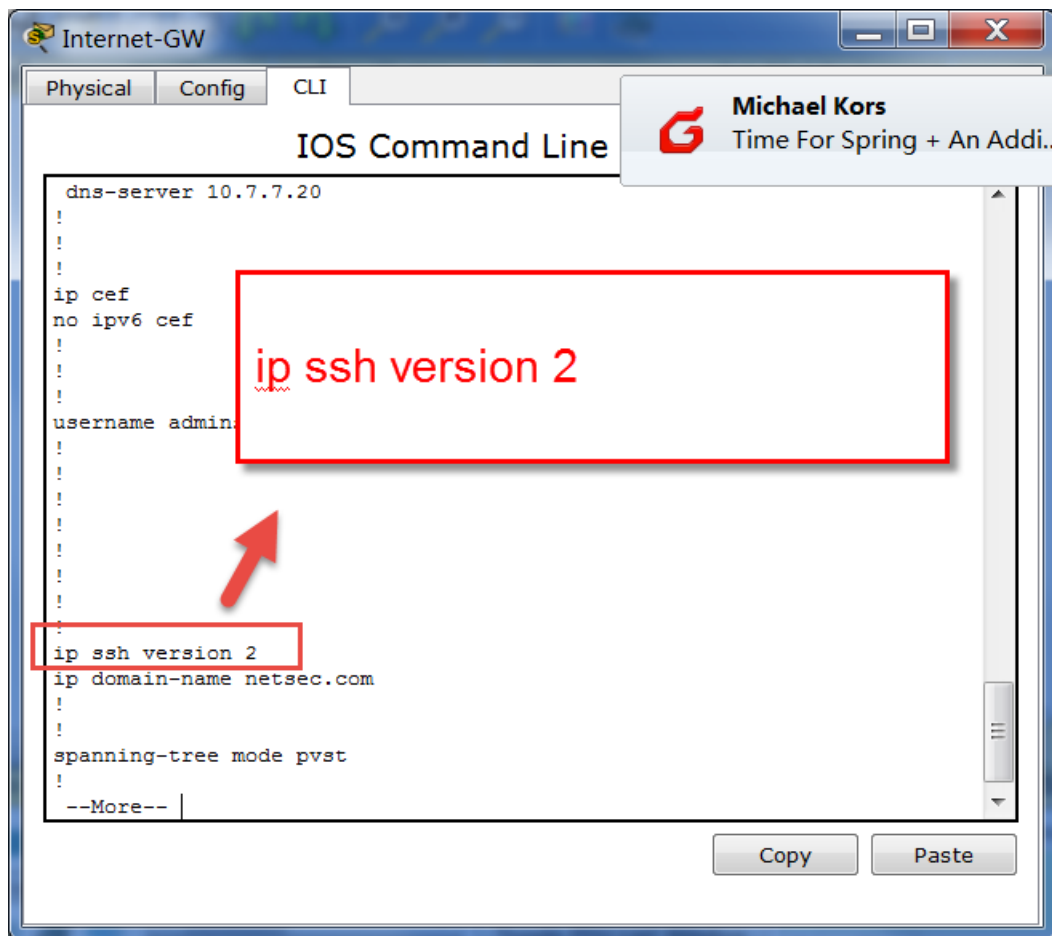


```
ciscoasa#conf t
Enter configuration commands, one per line. End with CNTRL-Z.
ciscoasa(config)#ip ssh version 2
Please create RSA keys (of at least 768 bits)
ciscoasa(config)#crypto key generate rsa
% You already have RSA keys defined named rsa
% Do you really want to replace them? [yes/no]: yes
The name for the keys will be: ciscoasa.netsec.com
Choose the size of the key modulus in the range of 768 to 4096:
General Purpose Keys. Choosing a key modulus of 2048 will
a few minutes.

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

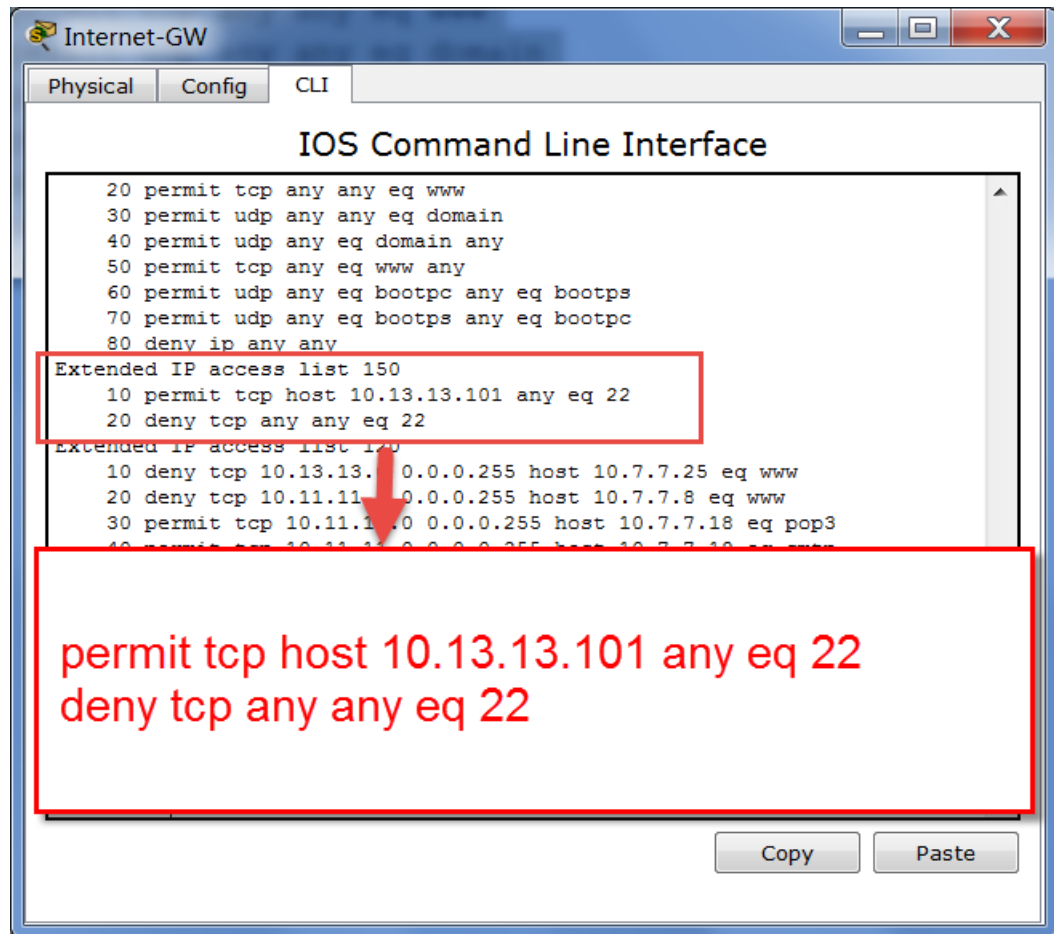
ciscoasa(config)#ip ssh version 2
??* 1 1:5:32.814: %SSH-5-ENABLED: SSH 1.99 has been enabled
ciscoasa(config)#
```

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

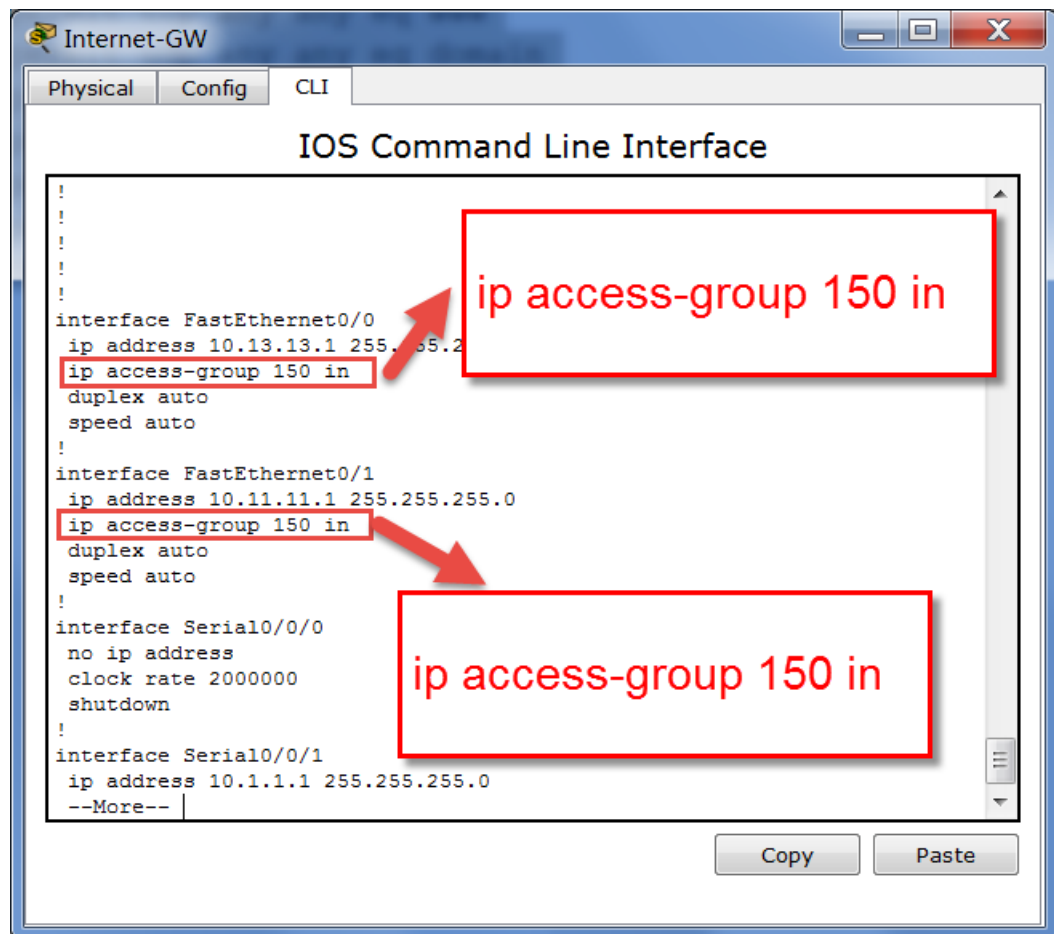


Description:

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

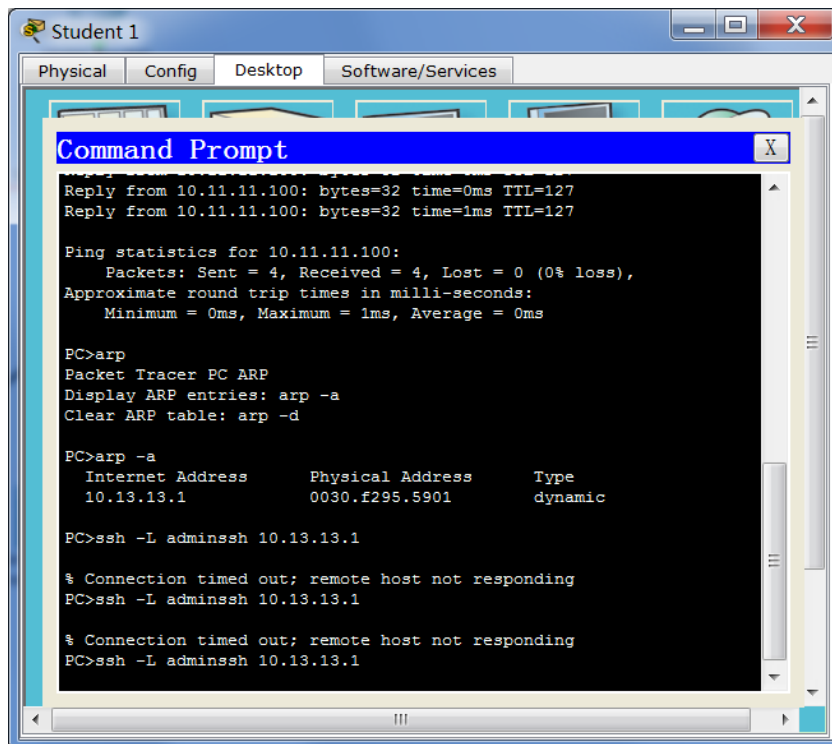
Deny tcp any 10.13.13.1 eq 22

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



Student 1

Physical Config Desktop Software/Services

Command Prompt

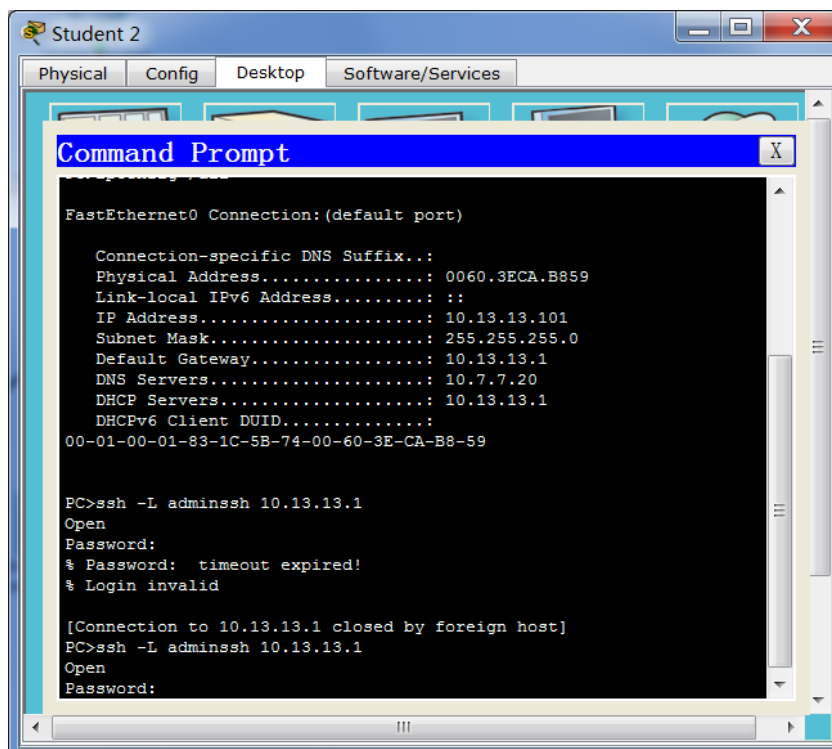
```
Reply from 10.11.11.100: bytes=32 time=0ms TTL=127
Reply from 10.11.11.100: bytes=32 time=1ms TTL=127

Ping statistics for 10.11.11.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>arp
Packet Tracer PC ARP
Display ARP entries: arp -a
Clear ARP table: arp -d

PC>arp -a
Internet Address      Physical Address      Type
10.13.13.1            0030.f295.5901        dynamic

PC>ssh -L adminssh 10.13.13.1
% Connection timed out; remote host not responding
PC>ssh -L adminssh 10.13.13.1
% Connection timed out; remote host not responding
PC>ssh -L adminssh 10.13.13.1
```



Student 2

Physical Config Desktop Software/Services

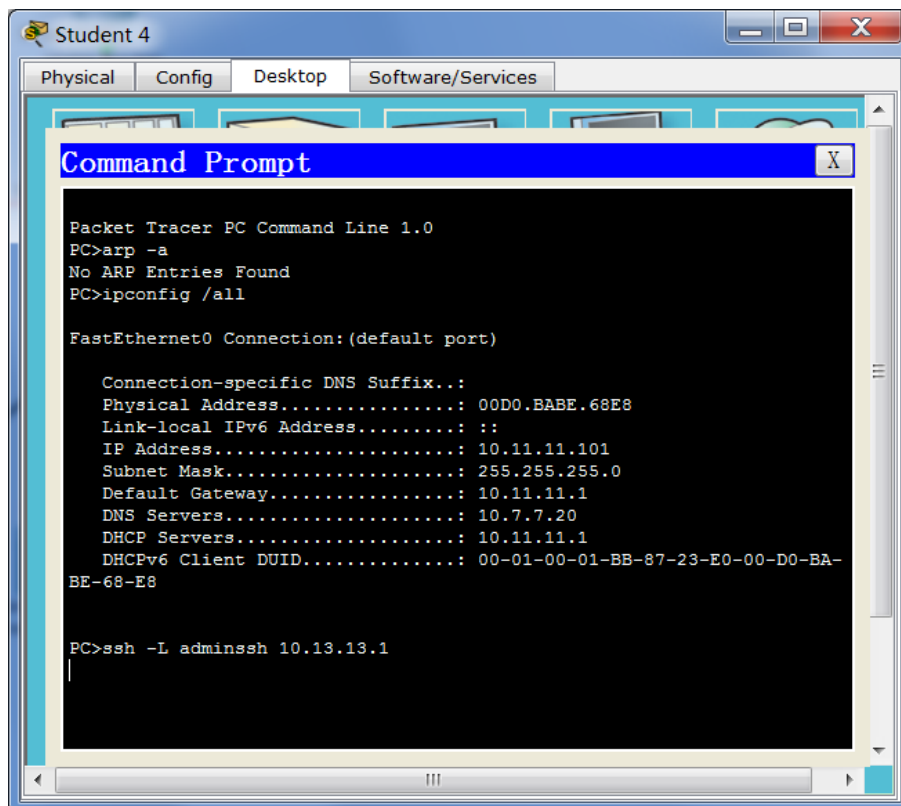
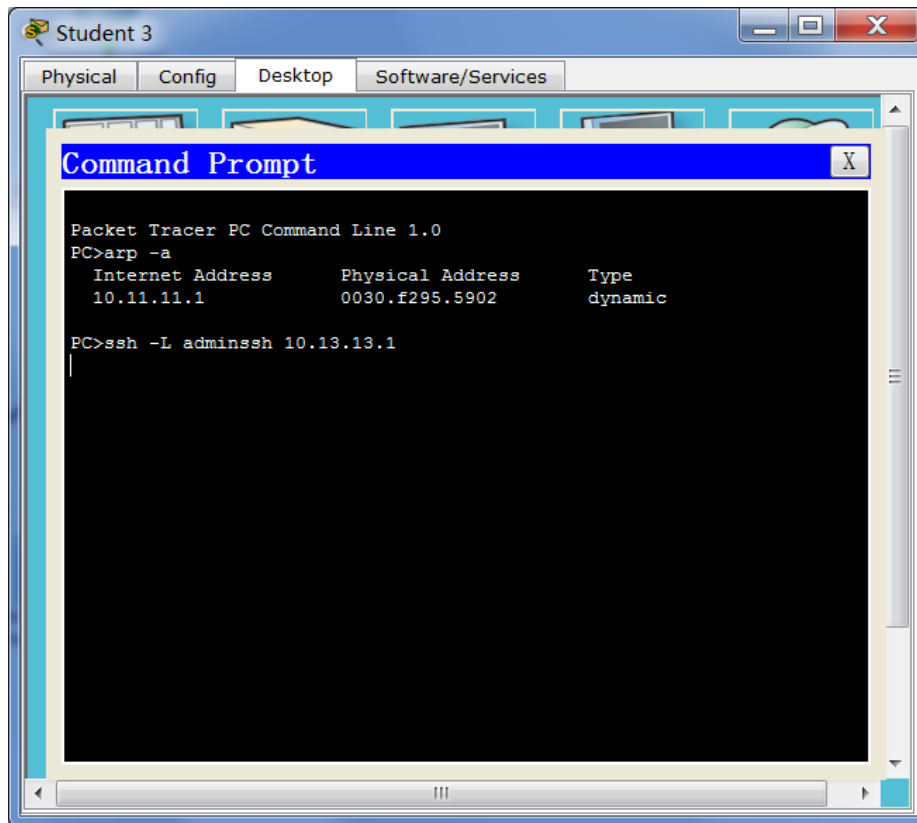
Command Prompt

```
FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix...:
Physical Address.....: 0060.3ECA.B859
Link-local IPv6 Address.....: ::
IP Address.....: 10.13.13.101
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 10.13.13.1
DNS Servers.....: 10.7.7.20
DHCP Servers.....: 10.13.13.1
DHCPv6 Client DUID.....:
00-01-00-01-83-1C-5B-74-00-60-3E-CA-B8-59

PC>ssh -L adminssh 10.13.13.1
Open
Password:
% Password: timeout expired!
% Login invalid

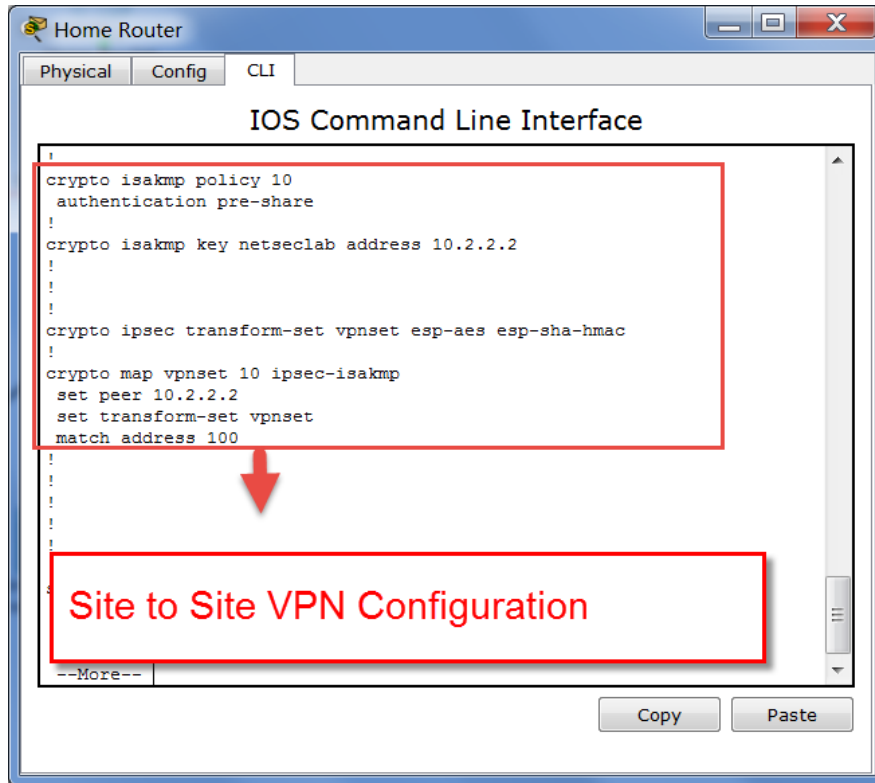
[Connection to 10.13.13.1 closed by foreign host]
PC>ssh -L adminssh 10.13.13.1
Open
Password:
```



Only student 2 can SSH.

3. Site-To-Site VPN settings.

1) VPN configuration



2) Results

