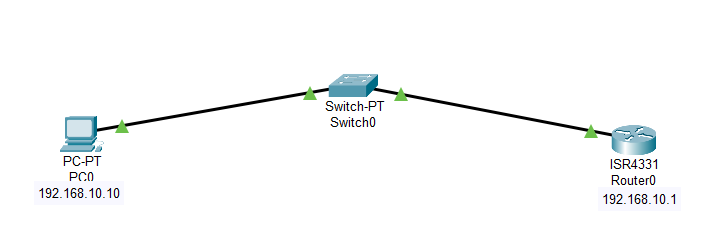
**Configuration and verification of remote user authentication on a Cisco router and switch using local username-password authentication using SSH.**



IPv4 Address:- 192.168.10.10 IPv4 Address:- 192.168.10.1

Gateway:- 192.168.10.1

CNSRouter#

CNSRouter#config t

CNSRouter(config)#hostname CNSRouter

CNSRouter(config)#enable password cisco

CNSRouter(config)#ip domain-name cisco.com

CNSRouter(config)#username Admin password cisco

CNSRouter(config)#cry?

CNSRouter(config)#crypto key generate RSA

How many bits in the modulus [512]: 1024

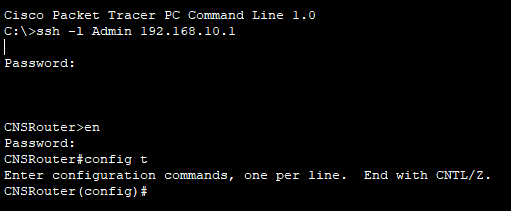
CNSRouter(config)#line vty 0 15

CNSRouter(config-line)#login local

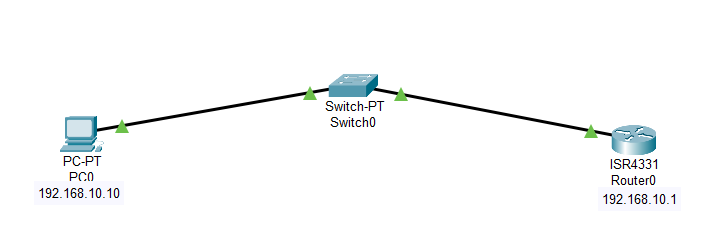
CNSRouter(config-line)#transport input SSH

CNSRouter(config-line)#exit

CNSRouter(config)#ip ssh version 2

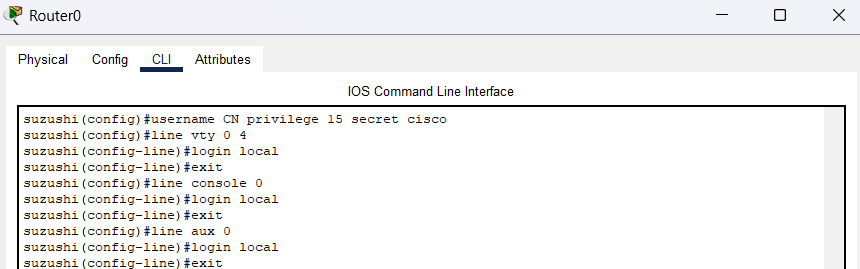


**Configuration and verification of remote user authentication on a Cisco router and switch using local username-password authentication.**



IPv4 Address:- 192.168.10.10 IPv4 Address:- 192.168.10.1

Gateway:- 192.168.10.1



suzushi (config) #username CN privilege 15 secret cisco

suzushi (config)#line vty 0 4

suzushi (config-line)#login local

suzushi (config-line)#exit

suzushi (config)#line console 0

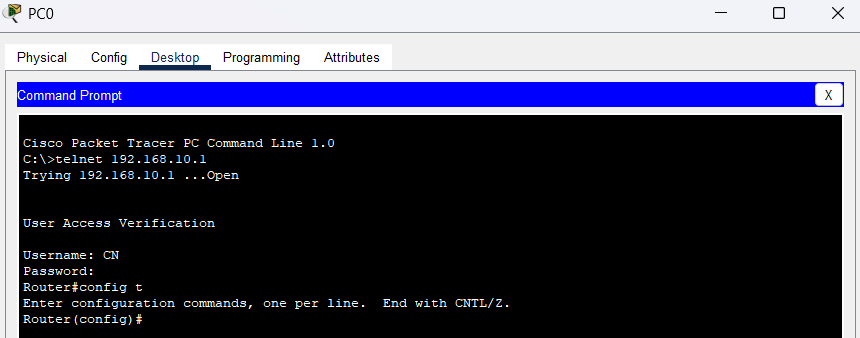
suzushi (config-line)#login local

suzushi (config-line)#exit

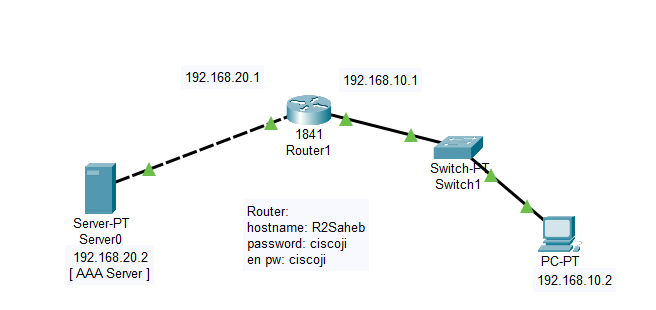
suzushi (config)#line aux 0

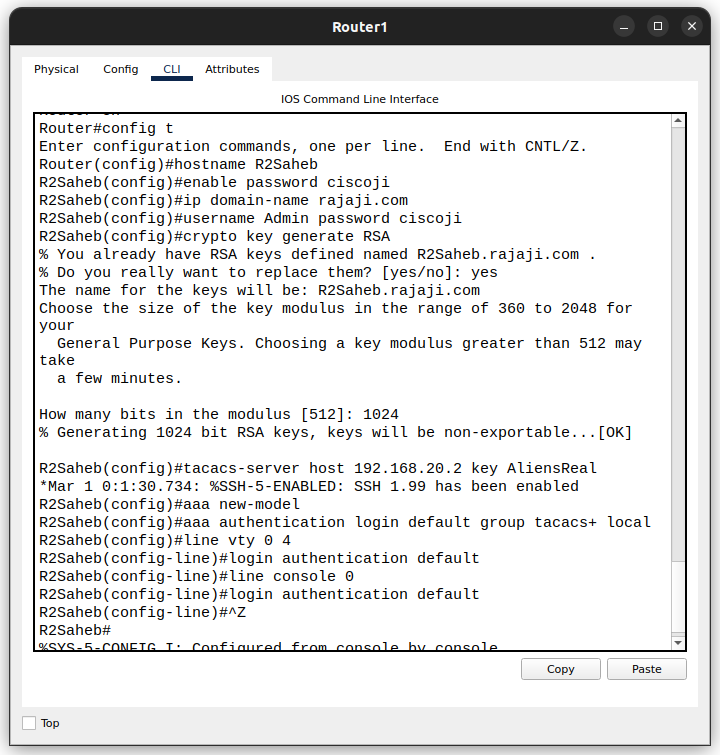
suzushi (config-line)#login local

suzushi (config-line)#exit.



**Configuration and verification of remote user authentication on a Cisco router using AAA server based username-password authentication.**





Router#config t

Enter configuration commands, one per line. End with CNTL/Z.

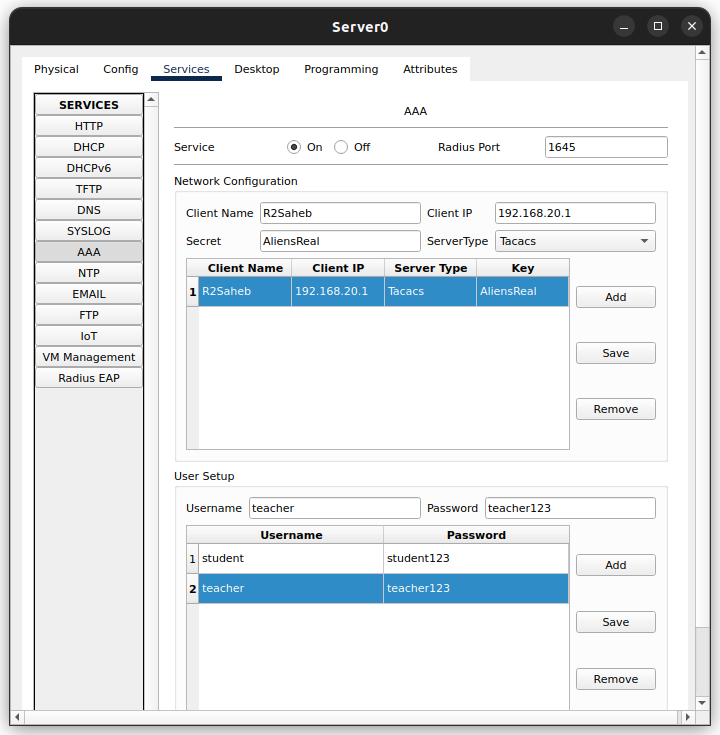
Router(config)#hostname R2Saheb

R2Saheb (config)#enable password ciscoji R2Saheb (config)#ip domain-name rajaji.com

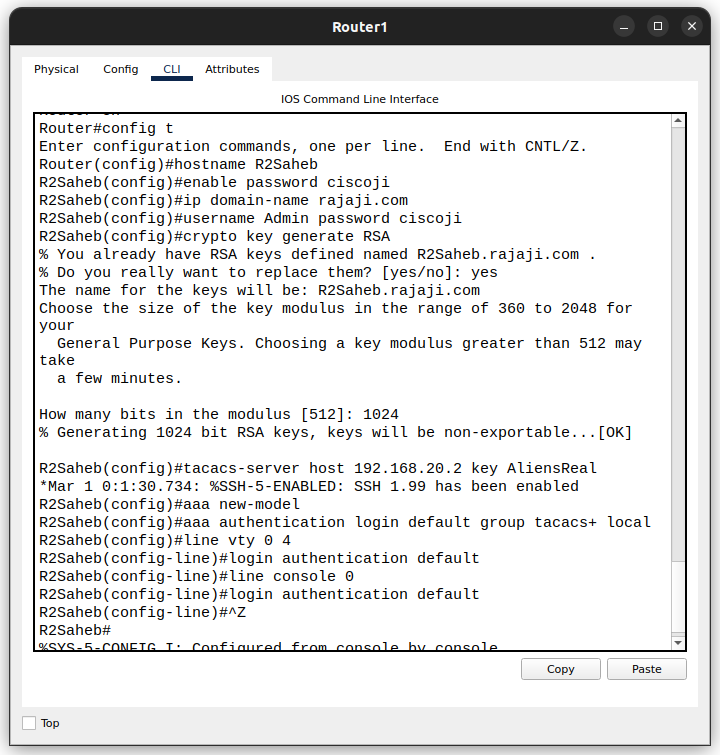
R2Saheb (config)#username Admin password ciscoji

R2Saheb(config)#crypto key generate RSA

GO to Service of server   
AAA



Router



R2Saheb (config)#tacacs-server host 192.168.20.2 key AliensReal \*Mar 1 0:1:30.734: %SSH-5-ENABLED: SSH 1.99 has been enabled

R2Saheb(config)#aaa new-model

R2Saheb(config)#aaa authentication login default group tacacs+ local

R2Saheb(config)#line vty 0 4

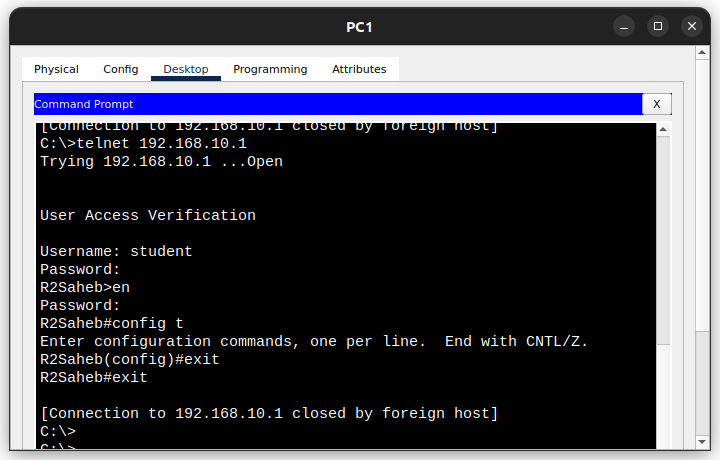
R2Saheb (config-line)#login authentication default

R2Saheb (config-line)#line console 0

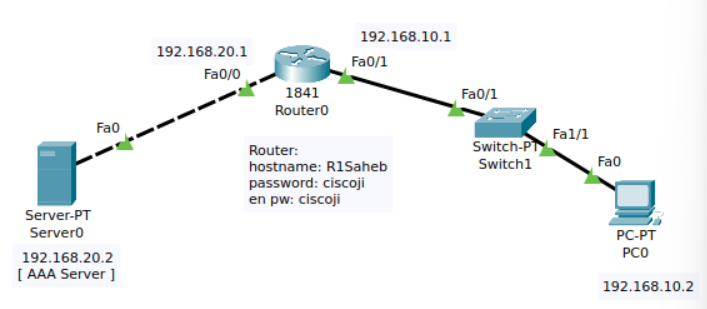
R2Saheb (config-line)#login authentication default

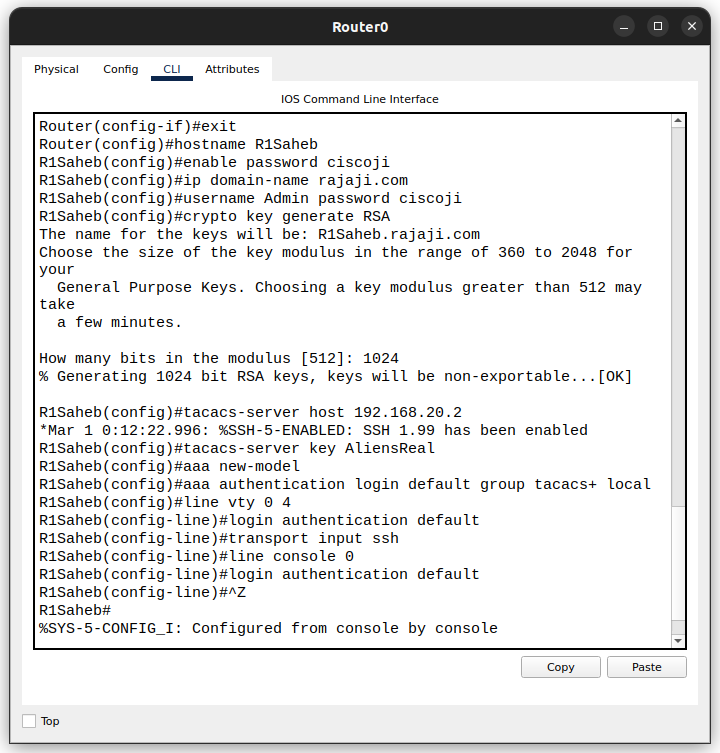
R2Saheb(config-line)#^Z

R2Saheb#



**Configuration and verification of remote user authentication on a Cisco router using AAA server based username-password authentication with SSH.**





Router(config-if)#exit

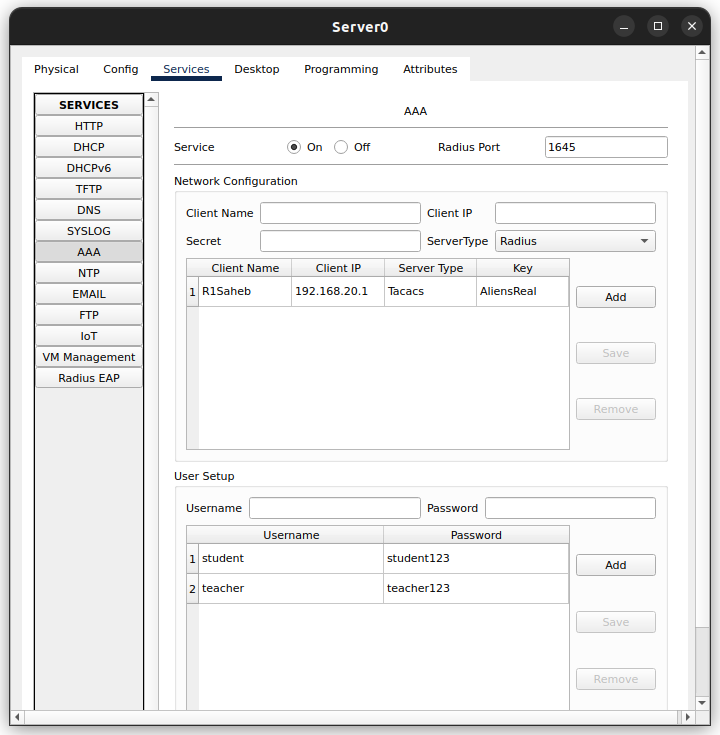
Router(config)#hostname R1Saheb

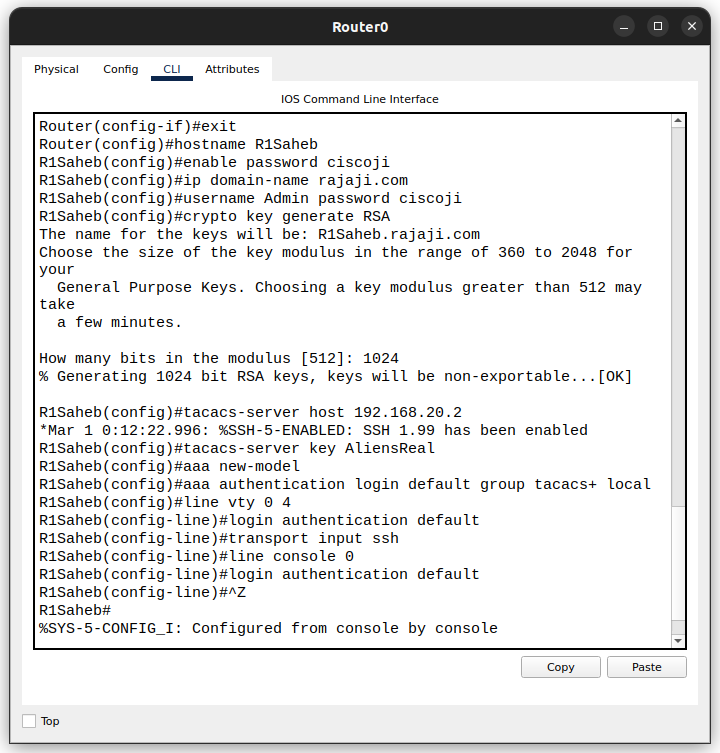
R1Saheb (config)#enable password ciscoji

R1Saheb(config)#ip domain-name rajaji.com

R1Saheb(config)#username Admin password ciscoji

R1Saheb(config)#crypto key generate RSA





R1Saheb(config)#tacacs-server host 192.168.20.2

\*Mar 1 0:12:22.996: %SSH-5-ENABLED: SSH 1.99 has been enabled

R1Saheb(config)#tacacs-server key AliensReal

R1Saheb(config)#aaa new-model

R1Saheb (config)#aaa authentication login default group tacacs+ local

R1Saheb (config)#line vty 0 4

R1Saheb(config-line)#login authentication default

R1Saheb (config-line)#transport input ssh

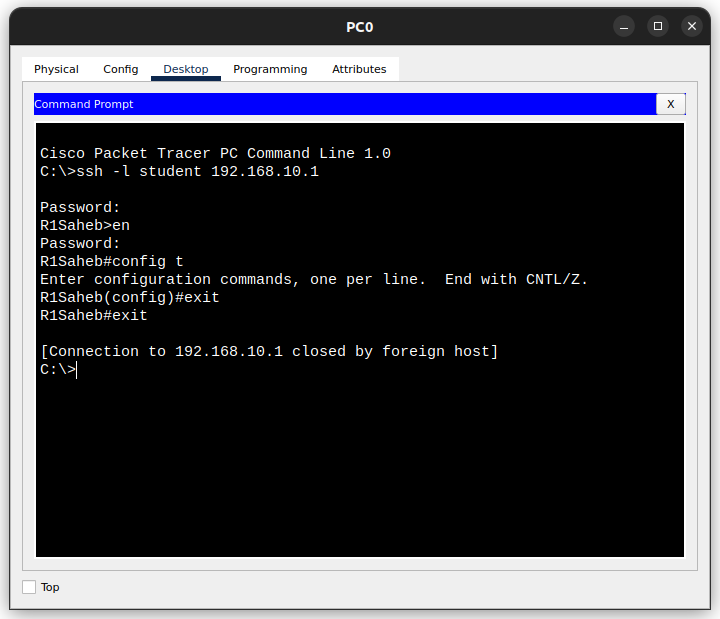
R1Saheb(config-line)#line console 0

R1Saheb(config-line)#login authentication default

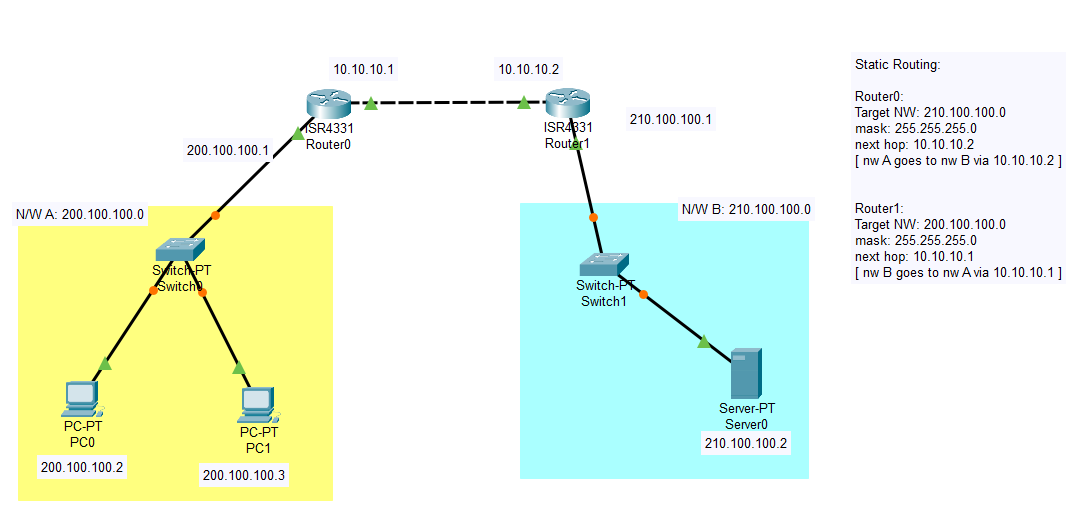
R1Saheb(config-line)#^Z

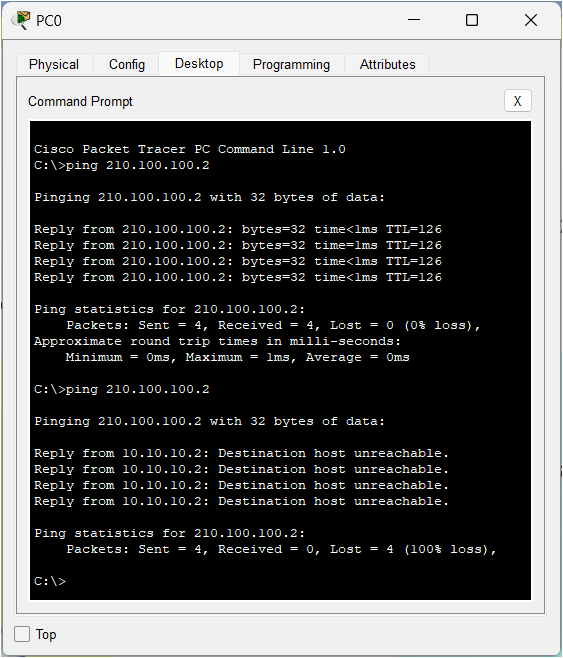
R1Saheb#

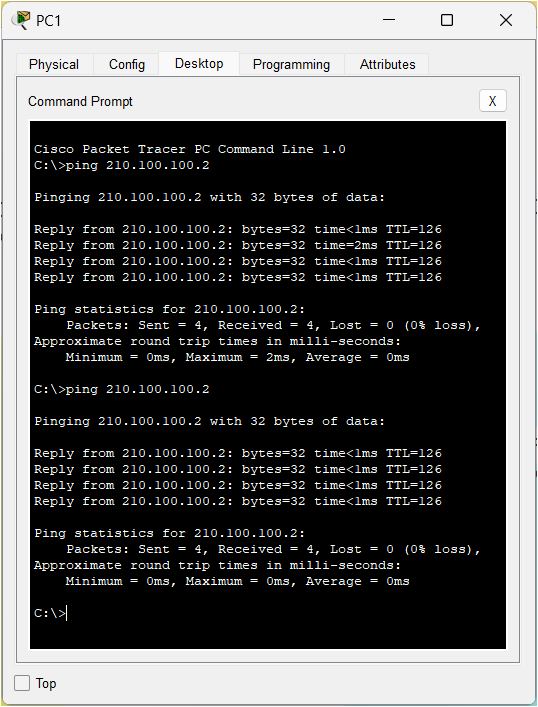
%SYS-5-CONFIG\_I: Configured from console by console

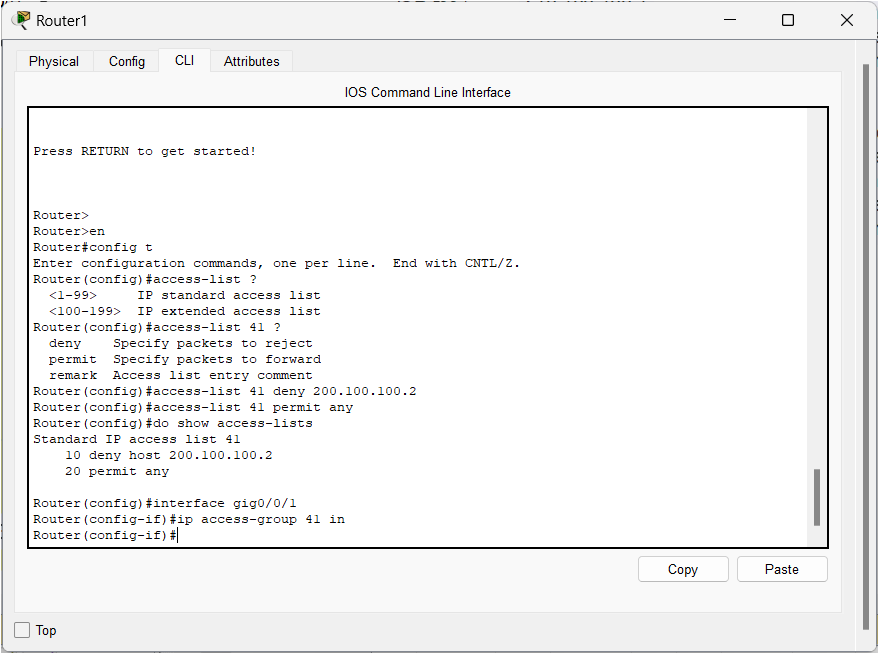


**Configuration and verification of a standard access list for permit and deny to a remote server.**









Router>

Router>en

Router config t

Enter configuration commands, one per line. End with CNTL/Z.

Router (config)#access-list?

Router (config)#access-list 41?

Router (config) #access-list 41 deny 200.100.100.2

Router (config)#access-list 41 permit any

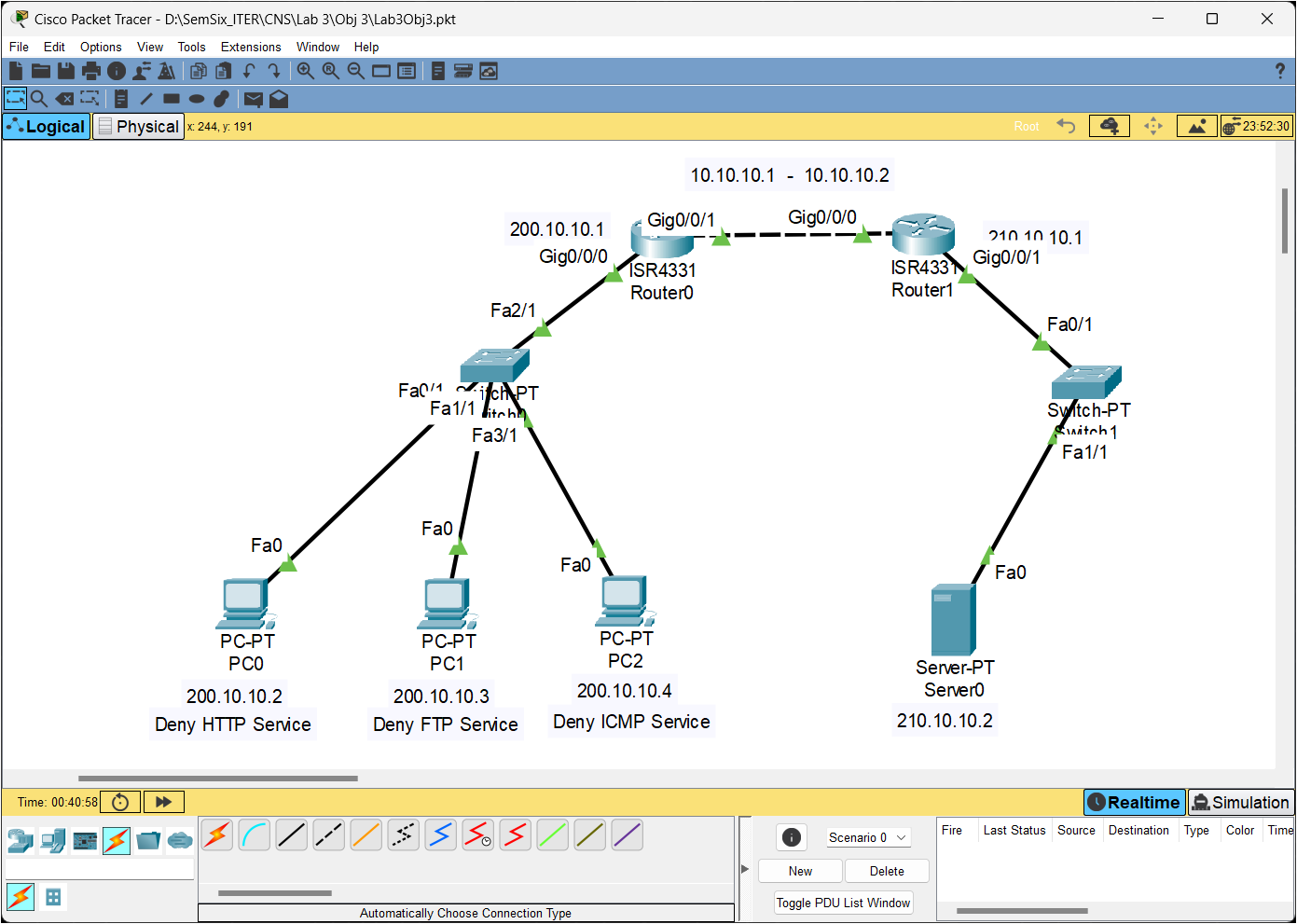
Router(config)#do show access-lists

Router (config)#interface gig0/0/1

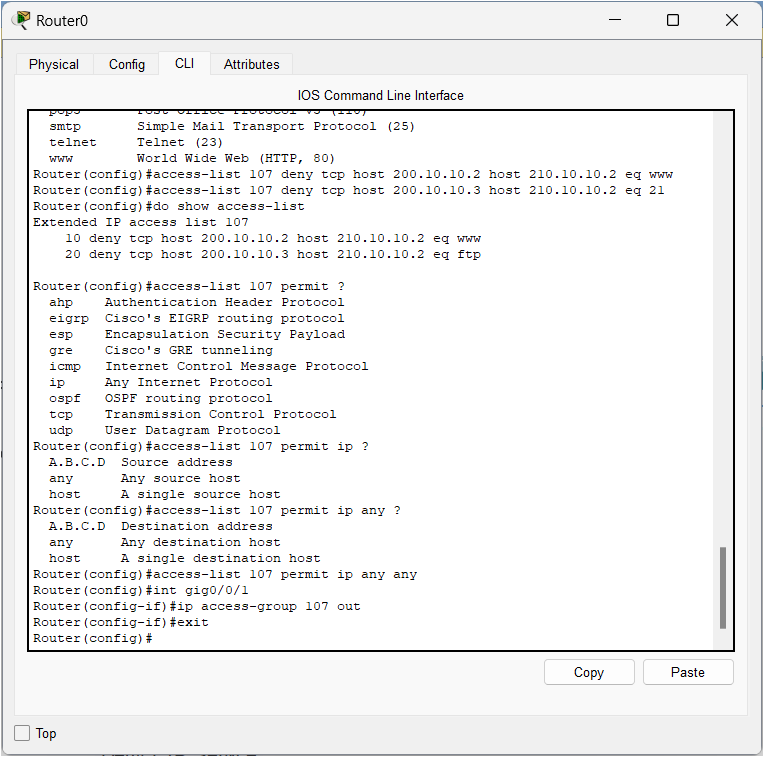
Router (config-if)#ip access-group 41 in

Router (config-if)#

**Configuration and verification of an extended access list for permit and deny to a remote server (HTTP/FTP).**



CLI FOR REMOTE SERVER



Router(config)#access-list 107 deny tep host 200.10.10.2 host 210.10.10.2 eq www.

Router(config)#access-list 107 deny top host 200.10.10.3 host 210.10.10.2 eq 21

Router(config)#do show access-list

Router(config)#access-list 107 permit?

Router (config)#access-list 107 permit ip?

Router(config)#access-list 107 permit ip any ?

Router(config)#access-list 107 permit ip any any

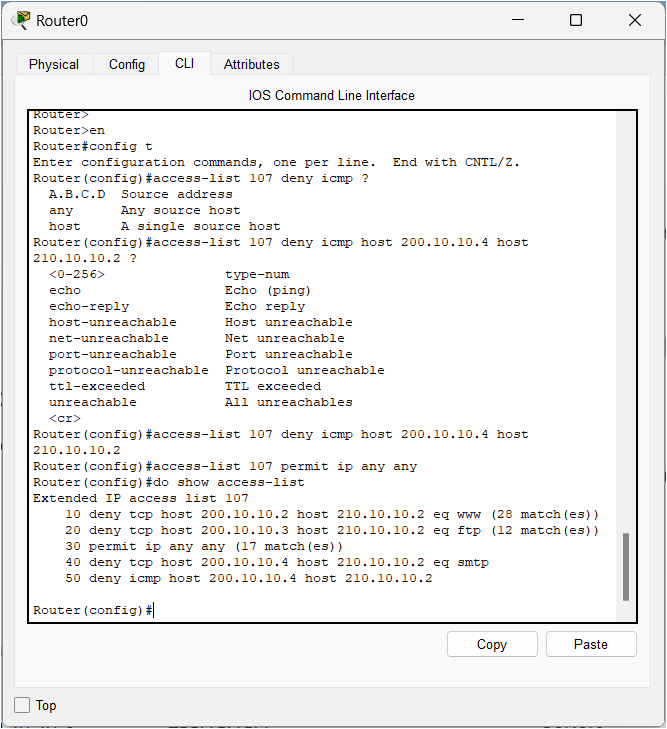
Router(config)#int gig0/0/1

Router(config-if)#ip access-group 107 out

Router(config-if)#exit

Router(config)#

CLI FOR ICMP



Router>

Router>en

Router#config t

Router (config) #access-list 107 deny icmp ?

Router(config)#access-list 107 deny icmp host 200.10.10.4 host

Router (config)#access-list 107 deny icmp host 200.10.10.4 host

210.10.10.2

Router (config) #access-list 107 permit ip any any

Router (config)#do show access-list

Router(config)#

