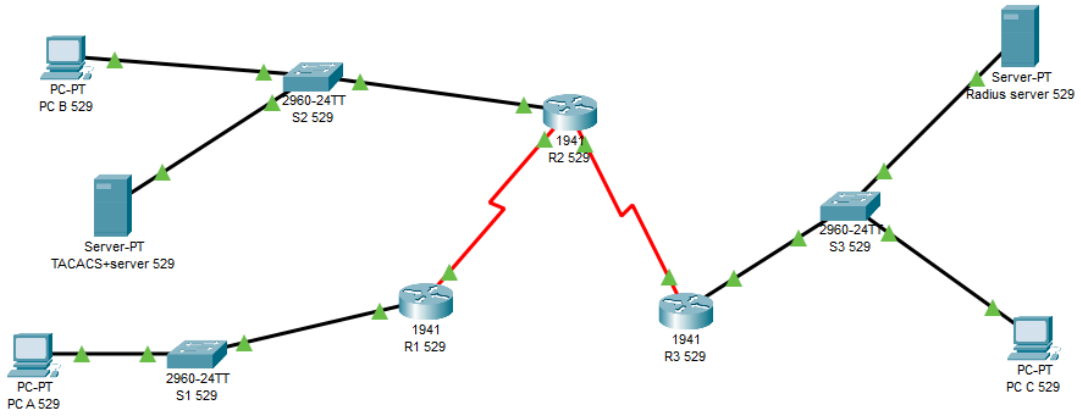
Practical No:2

Configure AAA Authentications.

Aim: a) Configure a local user account on Router and configure authenticate on the Console and vty lines using local AAA.

b) Verify local AAA authentication from the Router console and the PC-A client.

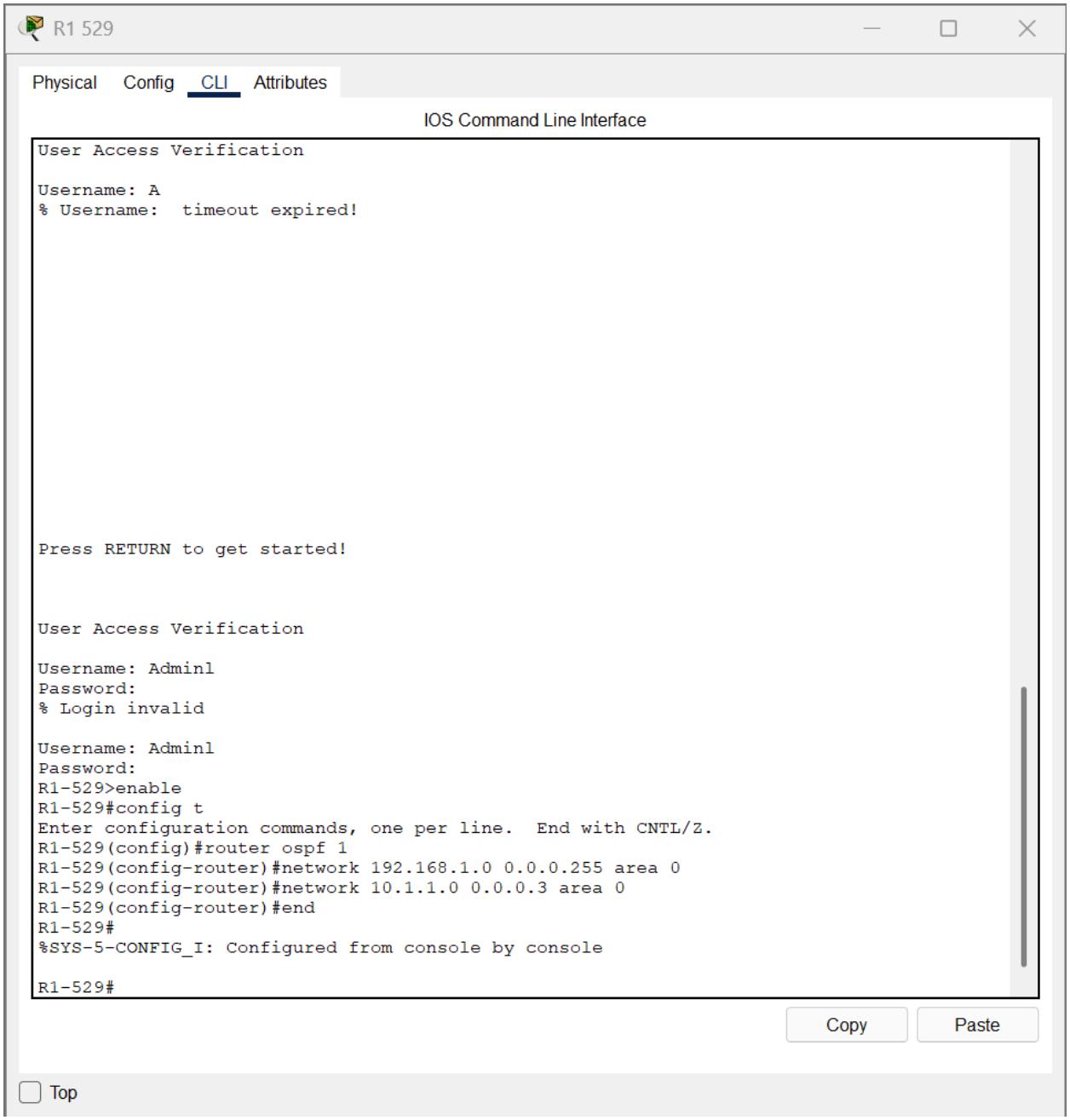
TOPOLOGY:

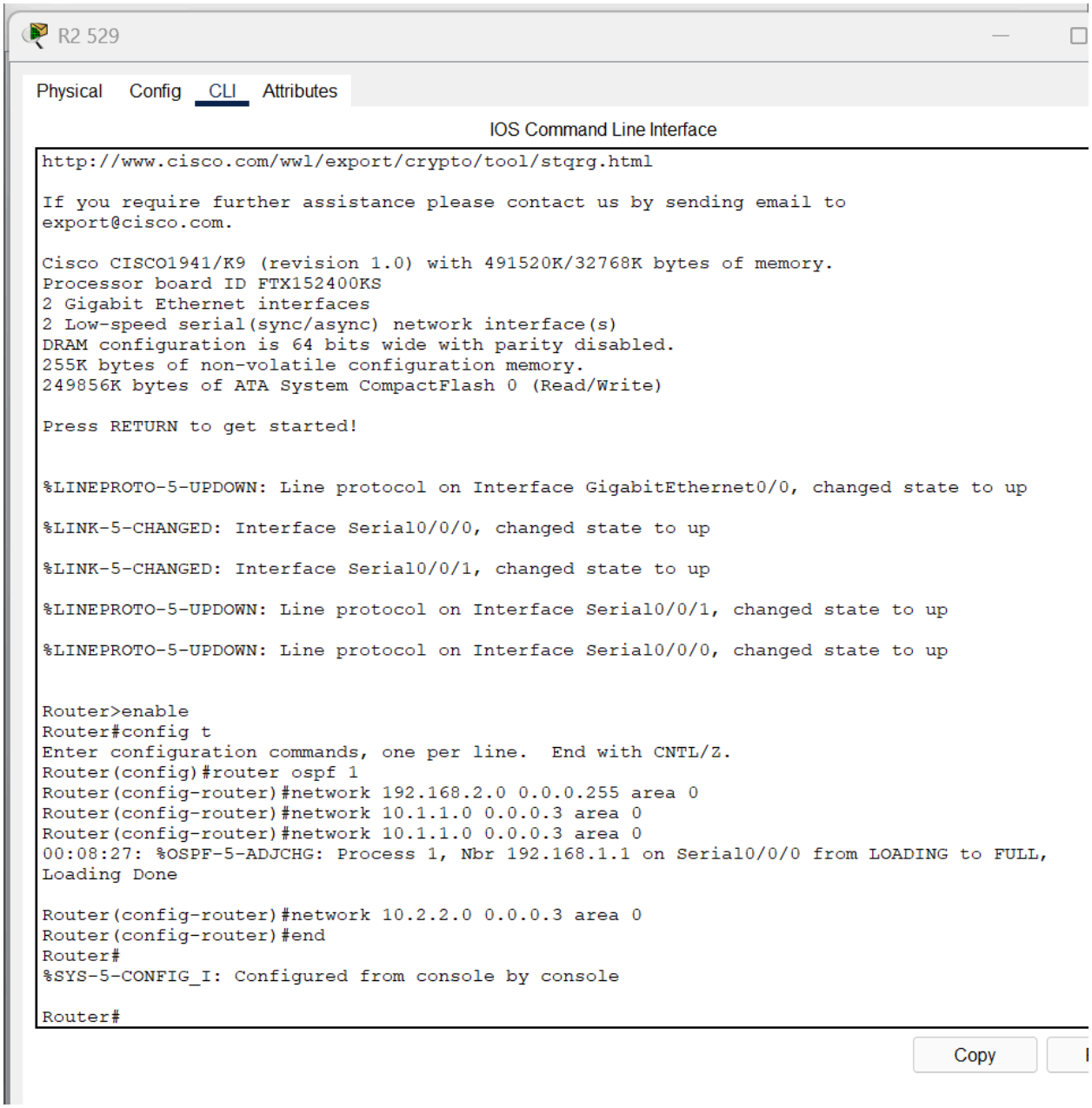


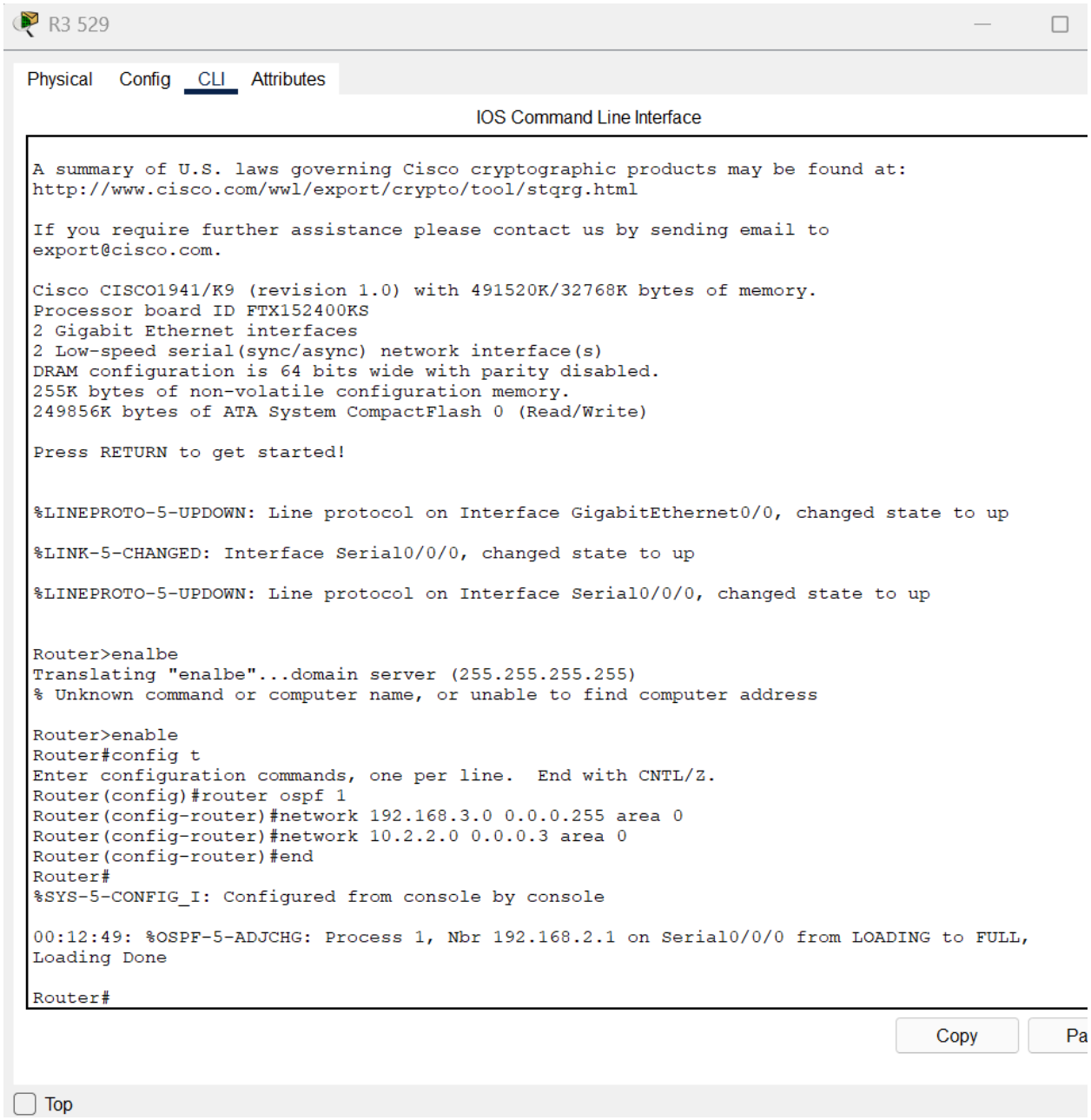
Addressing Table:

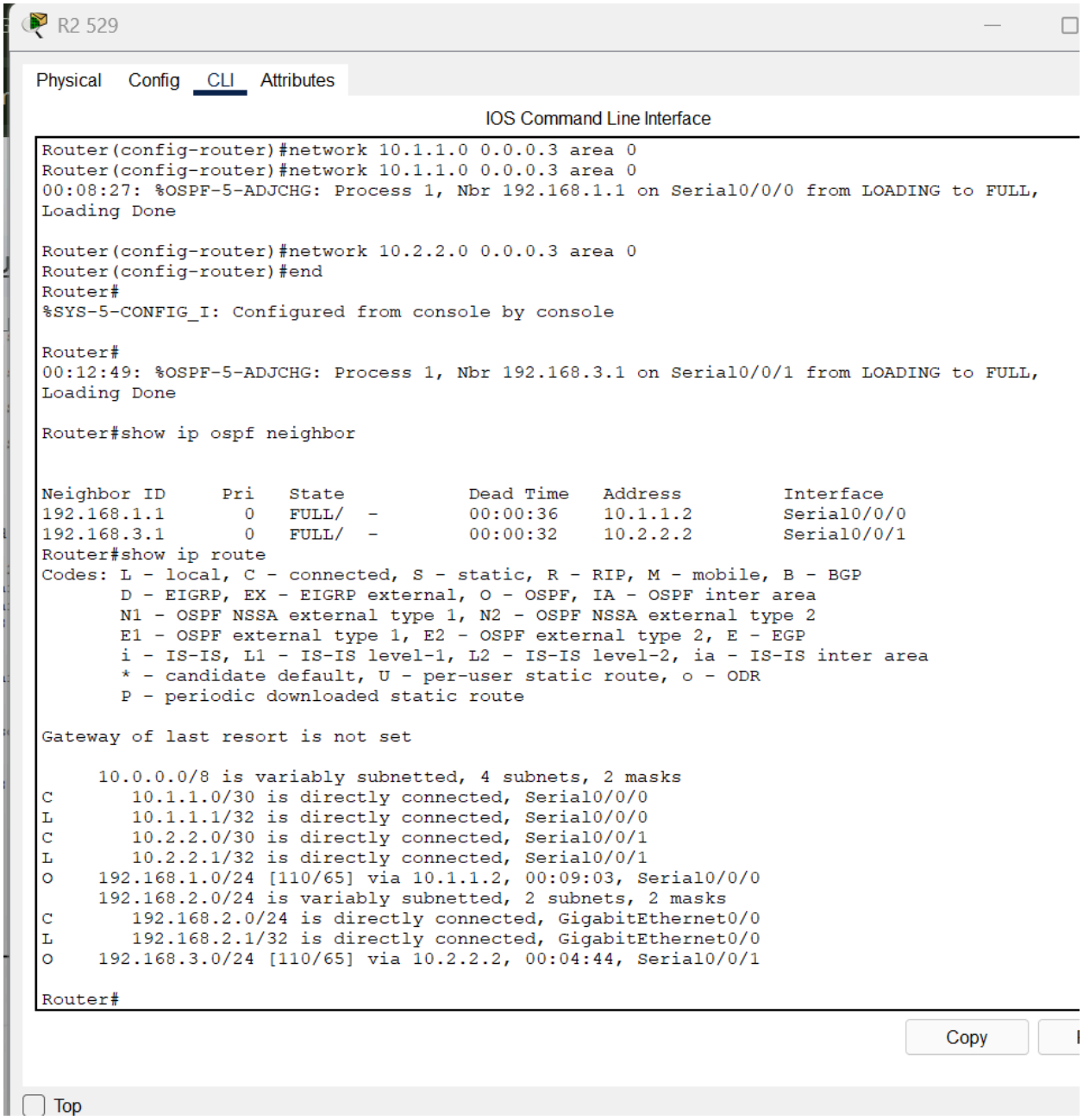
Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/1
	S0/0/0 (DCE)	10.1.1.2	255.255.255.252	N/A	N/A
R2	G0/0	192.168.2.1	255.255.255.0	N/A	S2 F0/2
	S0/0/0	10.1.1.1	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.1	255.255.255.252	N/A	N/A
R3	G0/1	192.168.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1	10.2.2.2	255.255.255.252	N/A	N/A
TACACS+ Server	NIC	192.168.2.2	255.255.255.0	192.168.2.1	S2 F0/6
RADIUS Server	NIC	192.168.3.2	255.255.255.0	192.168.3.1	S3 F0/1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/2
PC-B	NIC	192.168.2.3	255.255.255.0	192.168.2.1	S2 F0/1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

OSPF :

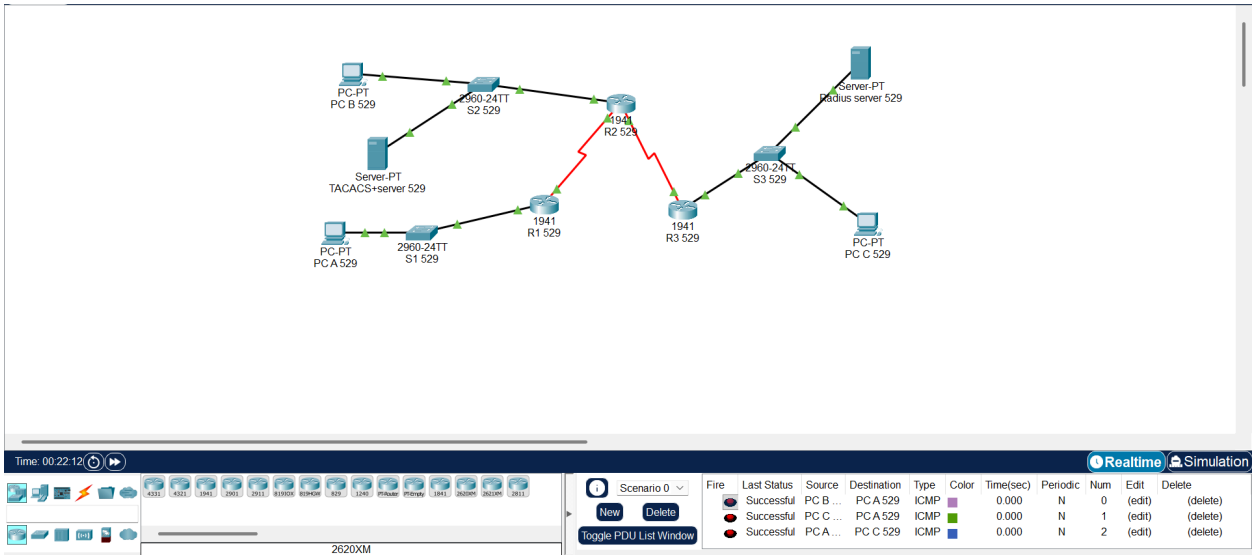

R1 529
Physical
Config
CLI
Attributes
IOS Command Line Interface
User Access Verification
Username: A
% Username: timeout expired!
Press RETURN to get started!
User Access Verification
Username: Adminl
Password:
% Login invalid
Username: Adminl
Password:
R1-529>enable
R1-529#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1-529(config)#router ospf 1
R1-529(config-router)#network 192.168.1.0 0.0.0.255 area 0
R1-529(config-router)#network 10.1.1.0 0.0.0.3 area 0
R1-529(config-router)#end
R1-529#
%SYS-5-CONFIG_I: Configured from console by console
R1-529#
Copy
Paste
Top


R2 529
Physical
Config
CLI
Attributes
IOS Command Line Interface
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to
export@cisco.com.
Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)
Press RETURN to get started!
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 192.168.2.0 0.0.0.255 area 0
Router(config-router)#network 10.1.1.0 0.0.0.3 area 0
Router(config-router)#network 10.1.1.0 0.0.0.3 area 0
00:08:27: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0 from LOADING to FULL,
Loading Done
Router(config-router)#network 10.2.2.0 0.0.0.3 area 0
Router(config-router)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#
Copy

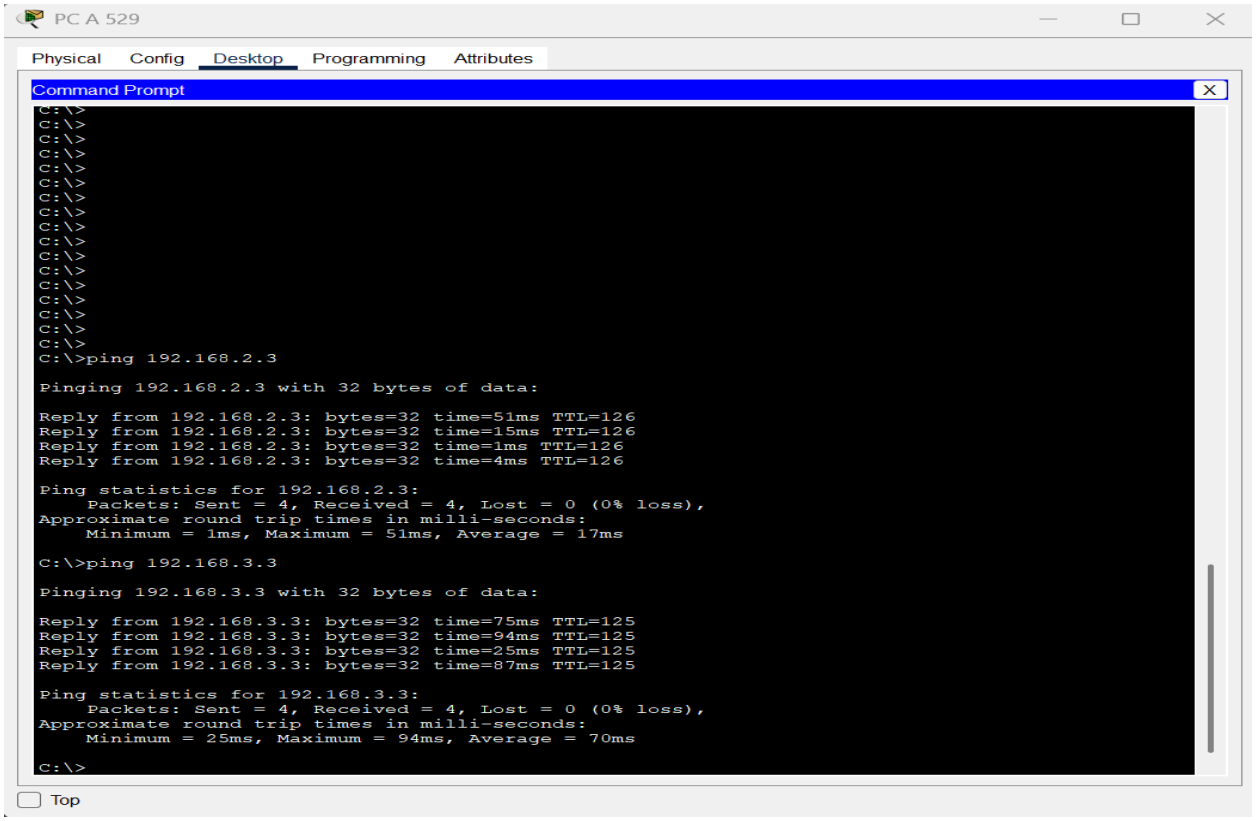

R3 529
Physical
Config
CLI
Attributes
IOS Command Line Interface
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to
export@cisco.com.
Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)
Press RETURN to get started!
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
Router>enalbe
Translating "enalbe"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 192.168.3.0 0.0.0.255 area 0
Router(config-router)#network 10.2.2.0 0.0.0.3 area 0
Router(config-router)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
00:12:49: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.2.1 on Serial0/0/0 from LOADING to FULL,
Loading Done
Router#
Copy
Pa
Top

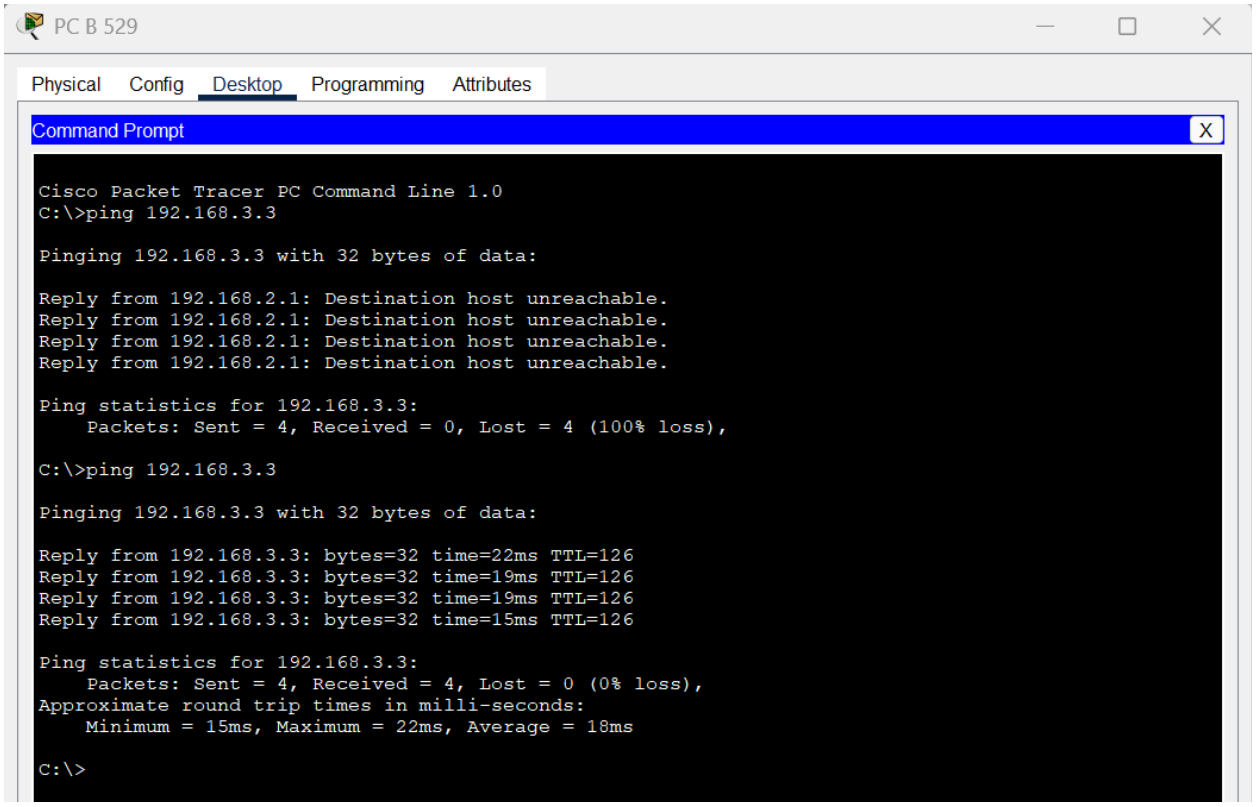

R2 529
Physical
Config
CLI
Attributes
IOS Command Line Interface
Router(config-router)#network 10.1.1.0 0.0.0.3 area 0
Router(config-router)#network 10.1.1.0 0.0.0.3 area 0
00:08:27: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0 from LOADING to FULL,
Loading Done
Router(config-router)#network 10.2.2.0 0.0.0.3 area 0
Router(config-router)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#
00:12:49: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.1 on Serial0/0/1 from LOADING to FULL,
Loading Done
Router#show ip ospf neighbor
Neighbor ID Pri State Dead Time Address Interface
192.168.1.1 0 FULL/ - 00:00:36 10.1.1.2 Serial0/0/0
192.168.3.1 0 FULL/ - 00:00:32 10.2.2.2 Serial0/0/1
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is not set
10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C 10.1.1.0/30 is directly connected, Serial0/0/0
L 10.1.1.1/32 is directly connected, Serial0/0/0
C 10.2.2.0/30 is directly connected, Serial0/0/1
L 10.2.2.1/32 is directly connected, Serial0/0/1
O 192.168.1.0/24 [110/65] via 10.1.1.2, 00:09:03, Serial0/0/0
192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.2.0/24 is directly connected, GigabitEthernet0/0
L 192.168.2.1/32 is directly connected, GigabitEthernet0/0
O 192.168.3.0/24 [110/65] via 10.2.2.2, 00:04:44, Serial0/0/1
Router#
Copy
Top

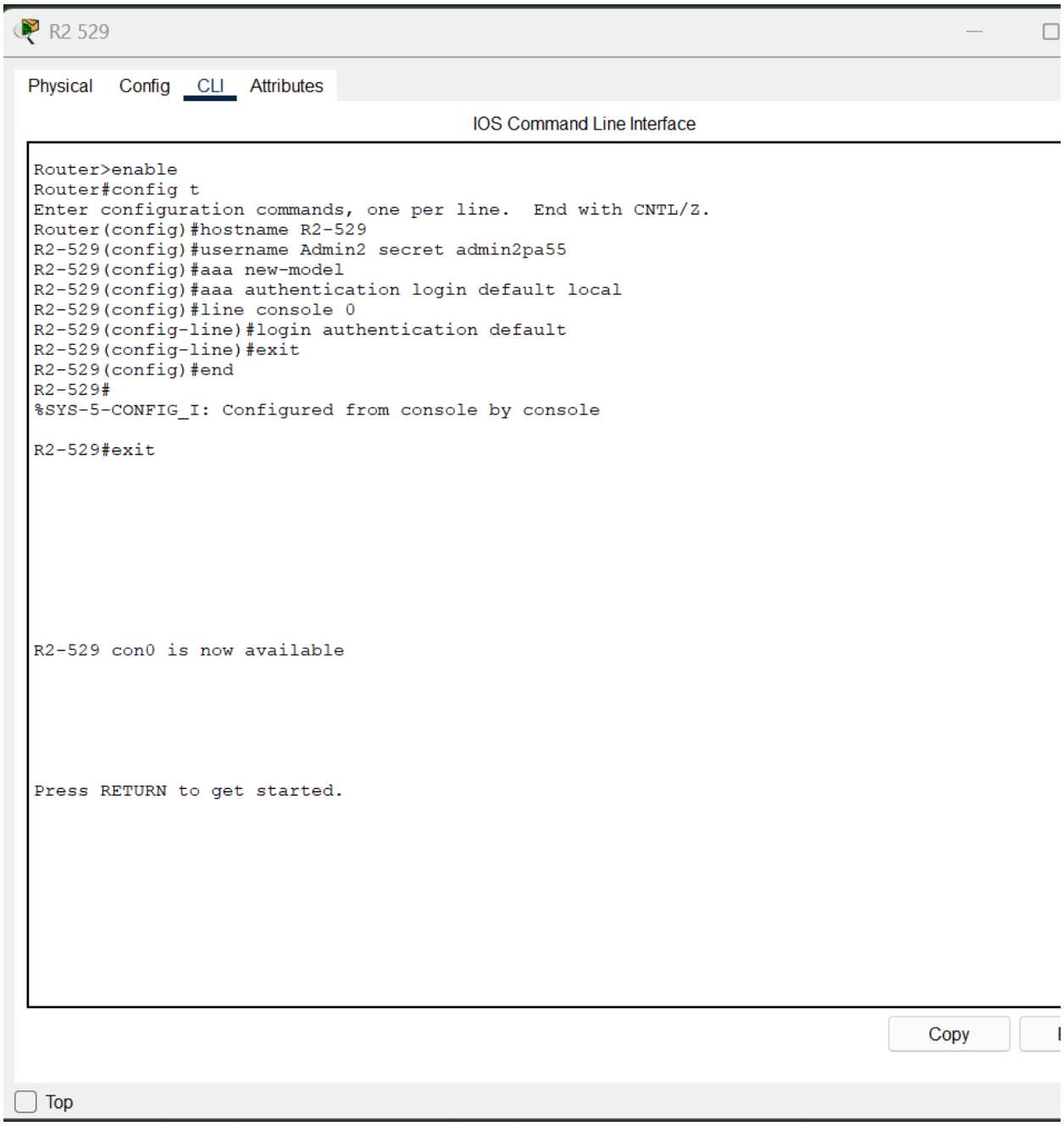
Packet Successful :

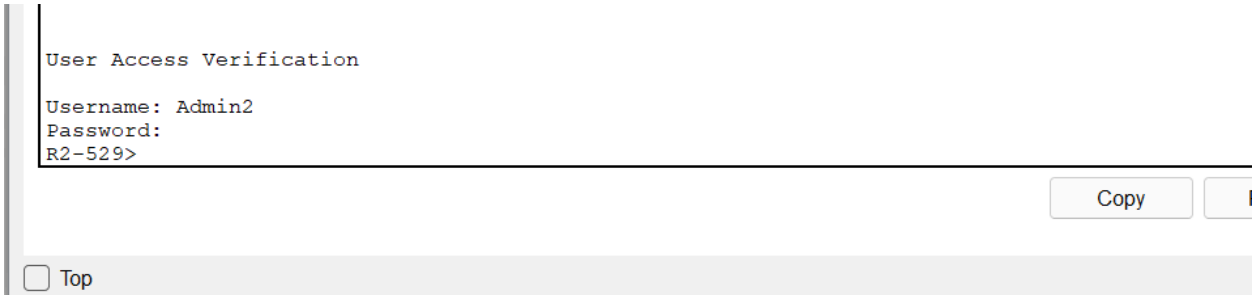


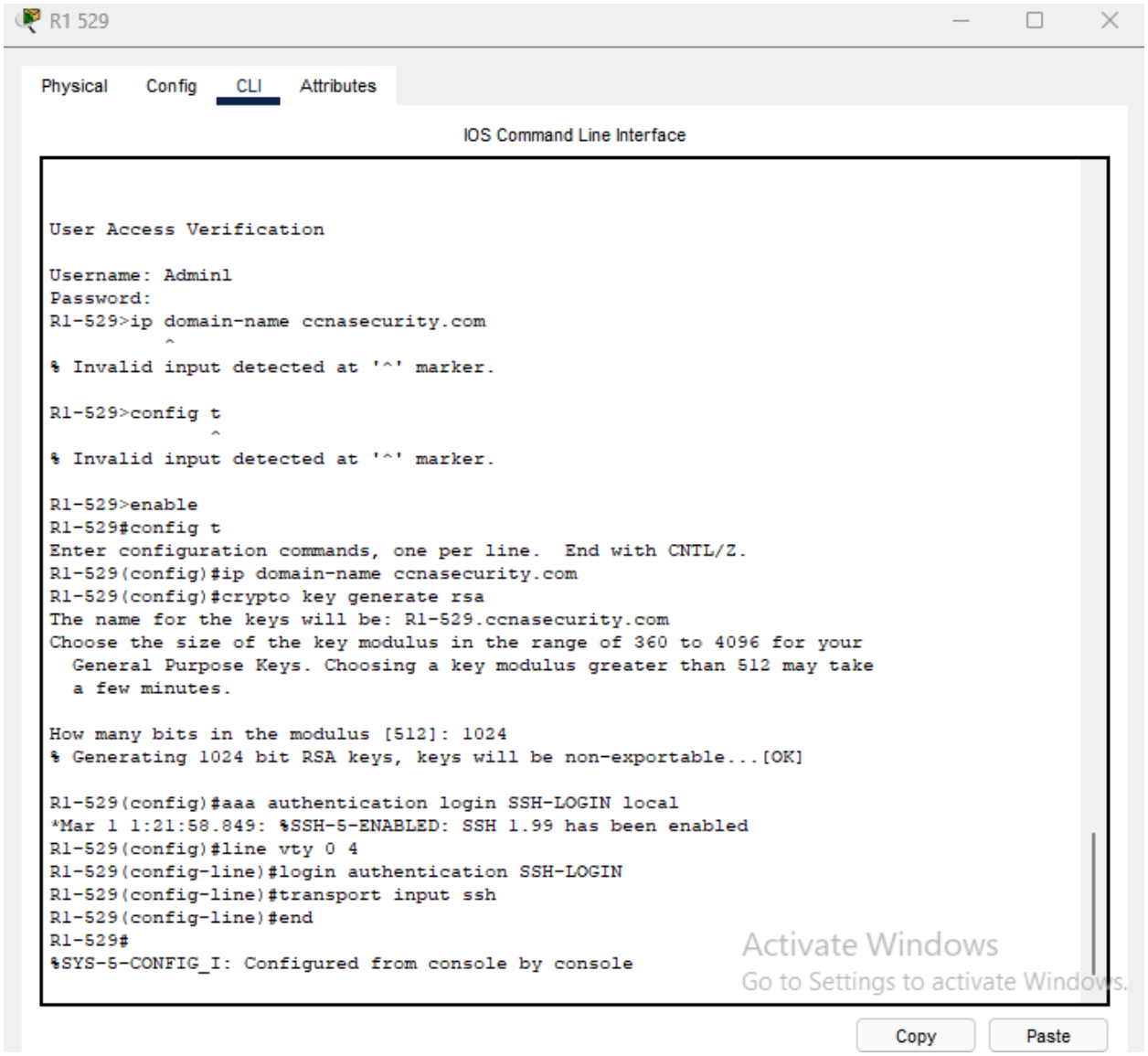
PING :

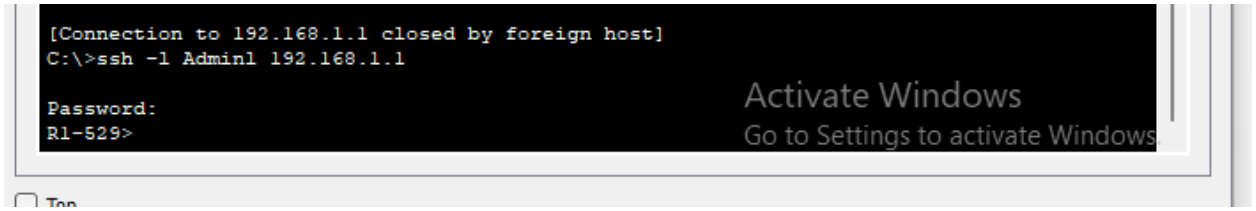



PC B 529
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.3
Pinging 192.168.3.3 with 32 bytes of data:
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Ping statistics for 192.168.3.3:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.3.3
Pinging 192.168.3.3 with 32 bytes of data:
Reply from 192.168.3.3: bytes=32 time=22ms TTL=126
Reply from 192.168.3.3: bytes=32 time=19ms TTL=126
Reply from 192.168.3.3: bytes=32 time=19ms TTL=126
Reply from 192.168.3.3: bytes=32 time=15ms TTL=126
Ping statistics for 192.168.3.3:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 15ms, Maximum = 22ms, Average = 18ms
C:\>


R2 529
Physical
Config
CLI
Attributes
IOS Command Line Interface
Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R2-529
R2-529(config)#username Admin2 secret admin2pa55
R2-529(config)#aaa new-model
R2-529(config)#aaa authentication login default local
R2-529(config)#line console 0
R2-529(config-line)#login authentication default
R2-529(config-line)#exit
R2-529(config)#end
R2-529#
%SYS-5-CONFIG_I: Configured from console by console
R2-529#exit
R2-529 con0 is now available
Press RETURN to get started.
Copy
Top


User Access Verification
Username: Admin2
Password:
R2-529>
Copy
Top


R1 529
Physical
Config
CLI
Attributes
IOS Command Line Interface
User Access Verification
Username: Adminl
Password:
R1-529>ip domain-name ccnasecurity.com
% Invalid input detected at '^' marker.
R1-529>config t
% Invalid input detected at '^' marker.
R1-529>enable
R1-529#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1-529(config)#ip domain-name ccnasecurity.com
R1-529(config)#crypto key generate rsa
The name for the keys will be: R1-529.ccnasecurity.com
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
R1-529(config)#aaa authentication login SSH-LOGIN local
*Mar 1 1:21:58.849: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1-529(config)#line vty 0 4
R1-529(config-line)#login authentication SSH-LOGIN
R1-529(config-line)#transport input ssh
R1-529(config-line)#end
R1-529#
%SYS-5-CONFIG_I: Configured from console by console
Activate Windows
Go to Settings to activate Windows.
Copy
Paste


[Connection to 192.168.1.1 closed by foreign host]
C:\>ssh -l Adminl 192.168.1.1
Password:
R1-529>
Activate Windows
Go to Settings to activate Windows

Part 3: Configure Server-Based AAA Authentication Using TACACS+ on R2.

```
User Access Verification

Username: Admin2
Password:
R2-529>
```

Copy

Top

TACACS+server 529

Physical Config Services Desktop Programming Attributes

SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP

AAA

Service On Off Radius Port 1645

Network Configuration

Client Name R2 Client IP 192.168.2.1

Secret tacacskey ServerType Tacacs

	Client Name	Client IP	Server Type	Key
1	R2	192.168.2.1	Tacacs	tacacskey

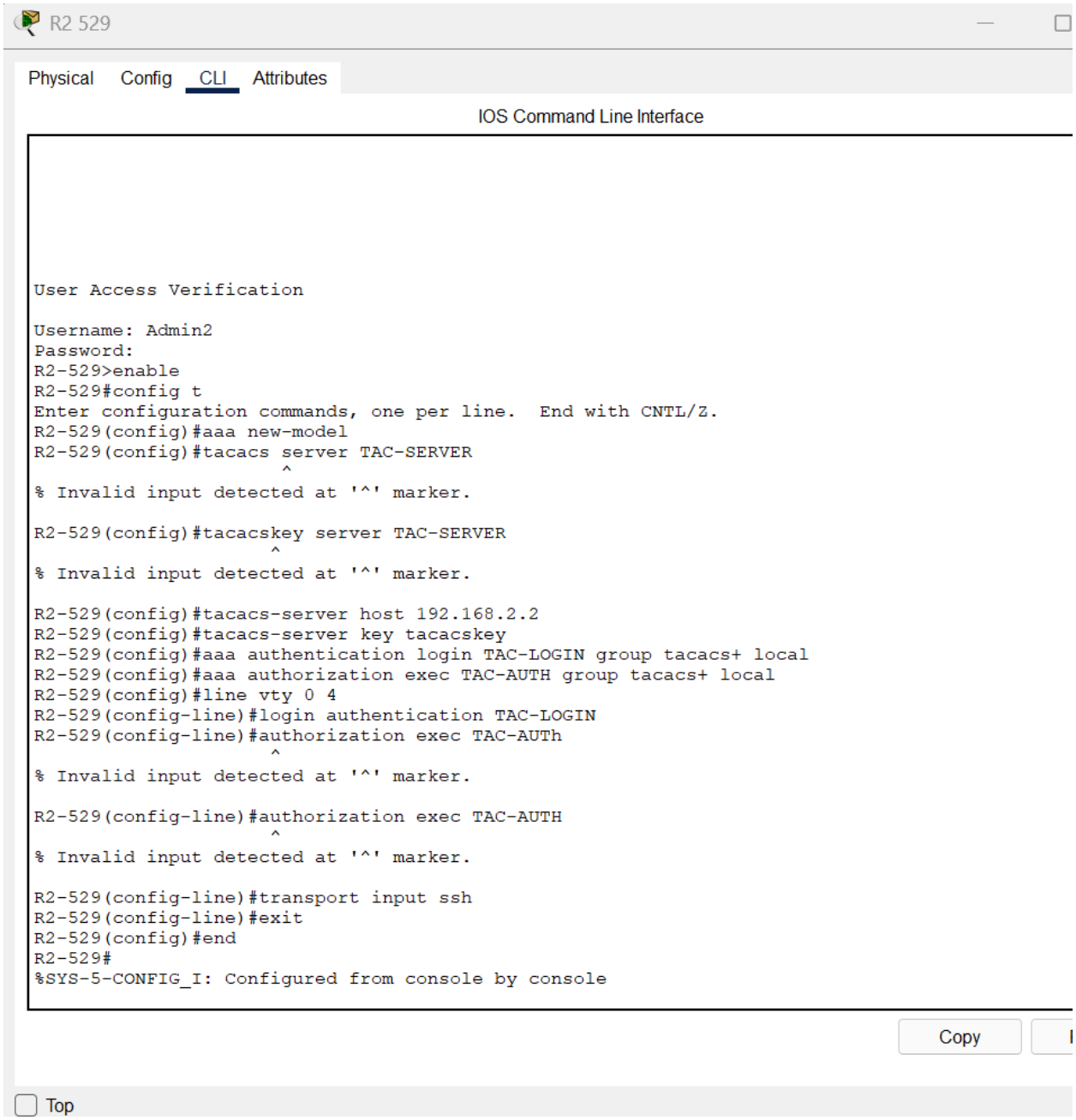
Add Save Remove

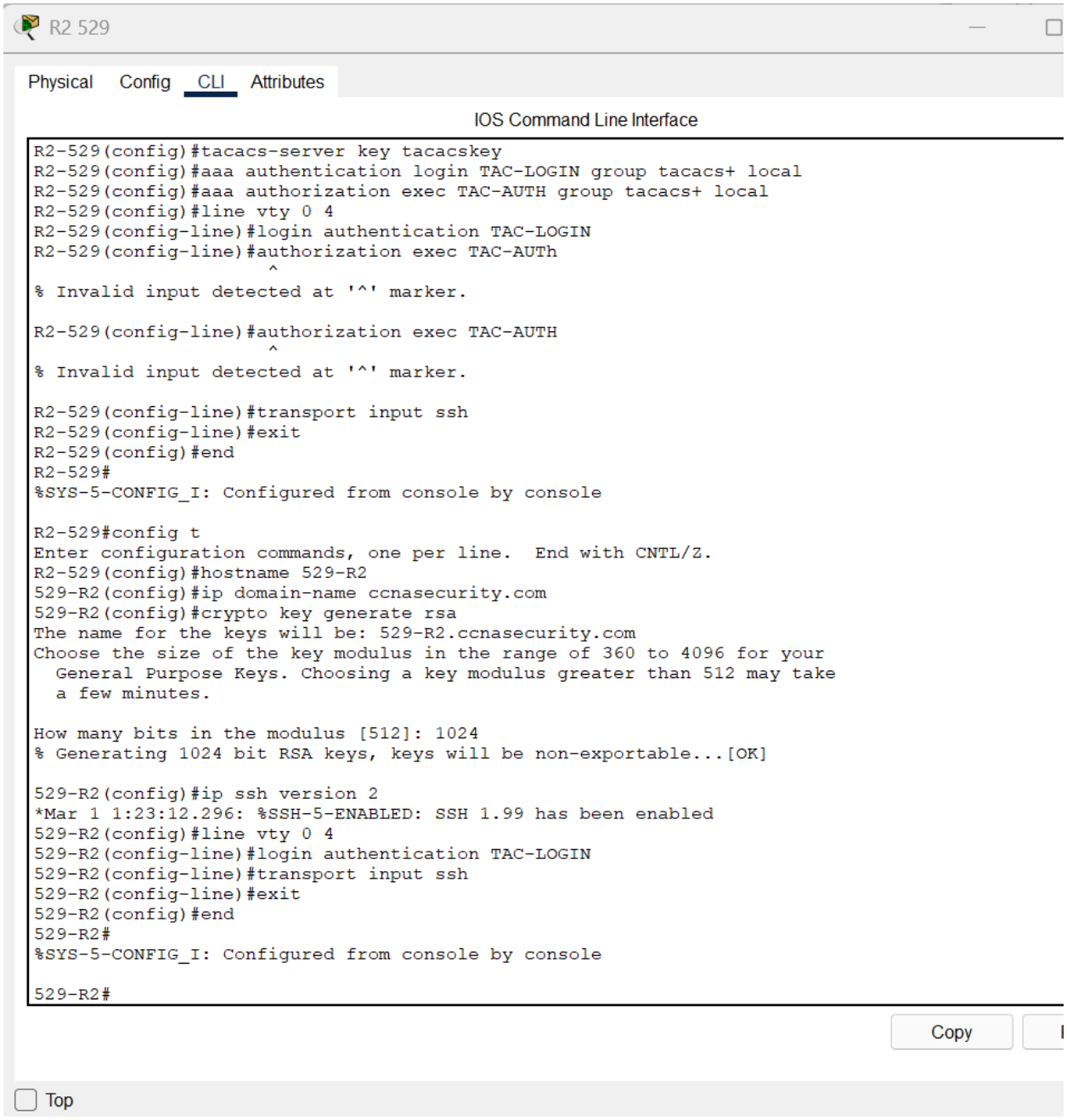
User Setup

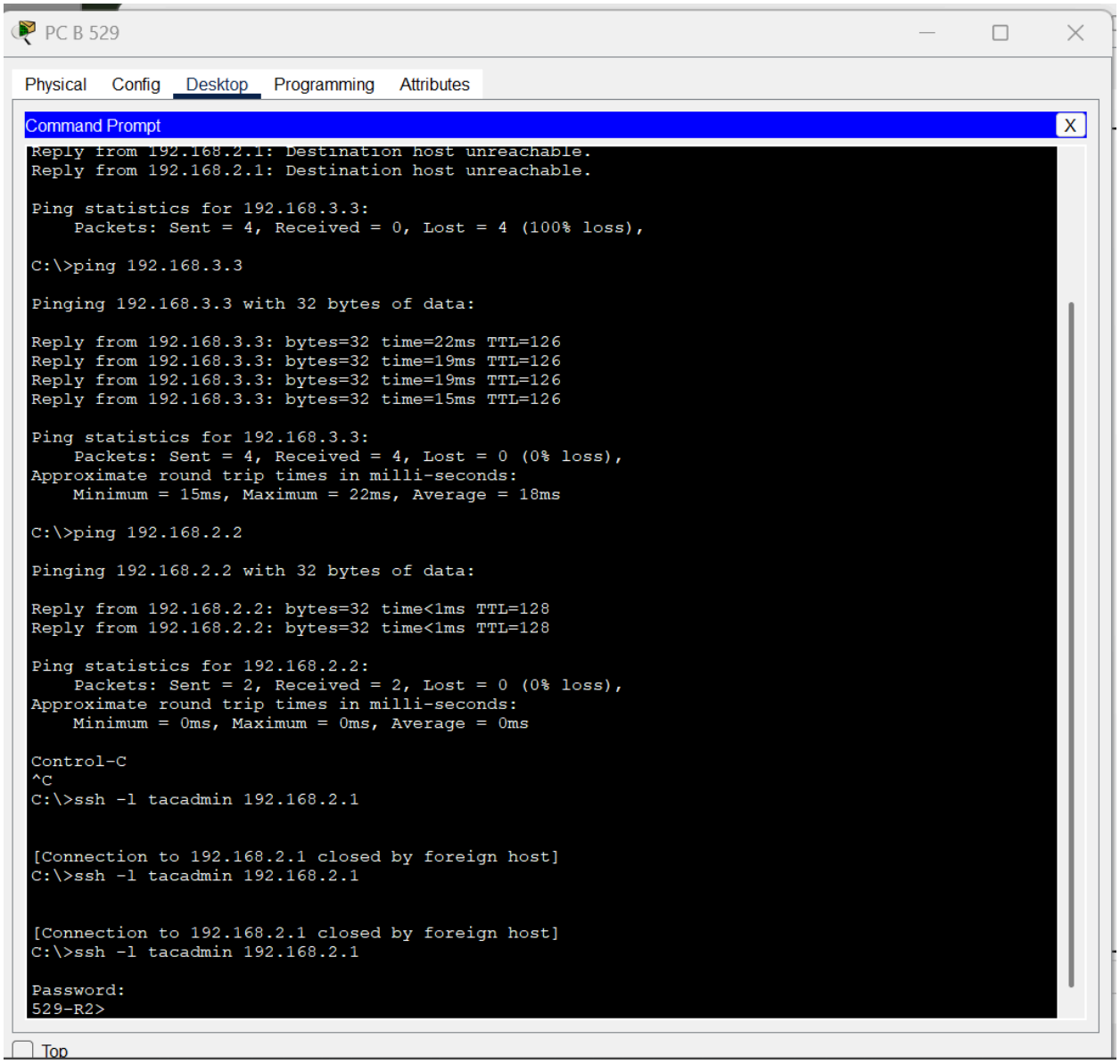
Username tacadmin Password tacpa55

	Username	Password
1	tacadmin	tacpa55

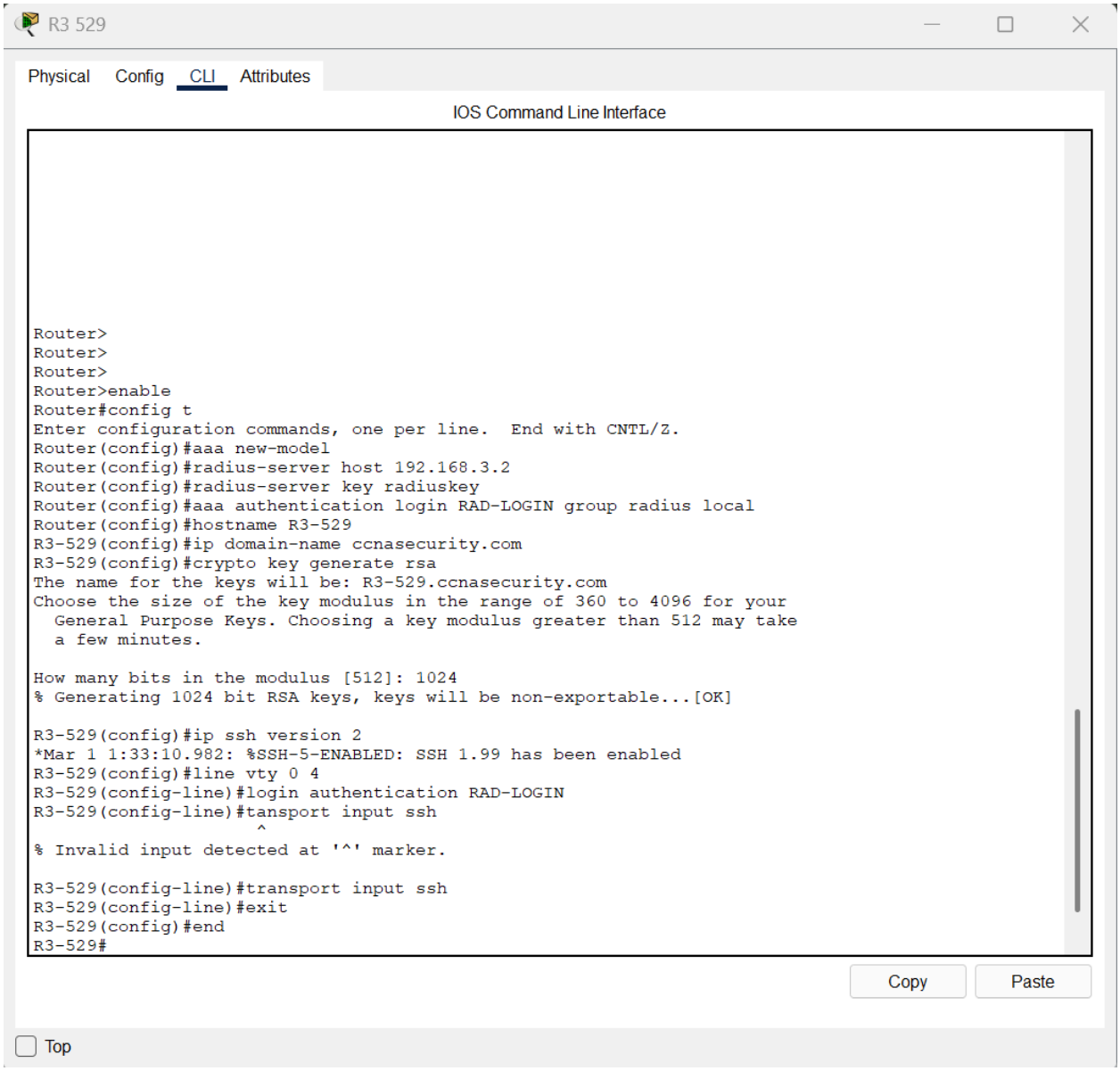
Add Save Remove

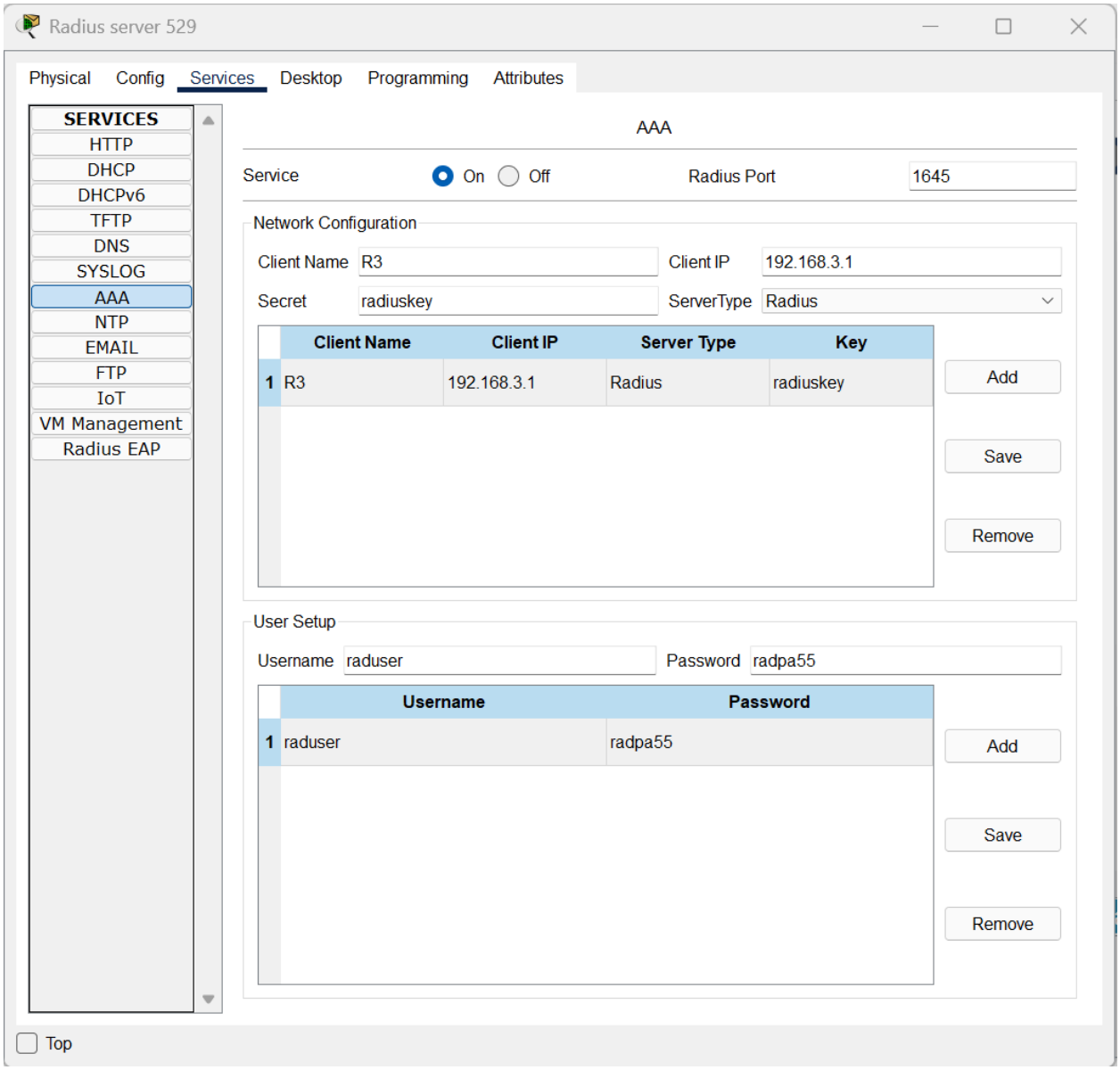

R2 529
Physical
Config
CLI
Attributes
IOS Command Line Interface
User Access Verification
Username: Admin2
Password:
R2-529>enable
R2-529#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2-529(config)#aaa new-model
R2-529(config)#tacacs server TAC-SERVER
                    ^
% Invalid input detected at '^' marker.
R2-529(config)#tacacskey server TAC-SERVER
                    ^
% Invalid input detected at '^' marker.
R2-529(config)#tacacs-server host 192.168.2.2
R2-529(config)#tacacs-server key tacacskey
R2-529(config)#aaa authentication login TAC-LOGIN group tacacs+ local
R2-529(config)#aaa authorization exec TAC-AUTH group tacacs+ local
R2-529(config)#line vty 0 4
R2-529(config-line)#login authentication TAC-LOGIN
R2-529(config-line)#authorization exec TAC-AUTh
                    ^
% Invalid input detected at '^' marker.
R2-529(config-line)#authorization exec TAC-AUTH
                    ^
% Invalid input detected at '^' marker.
R2-529(config-line)#transport input ssh
R2-529(config-line)#exit
R2-529(config)#end
R2-529#
%SYS-5-CONFIG_I: Configured from console by console
Copy
Top

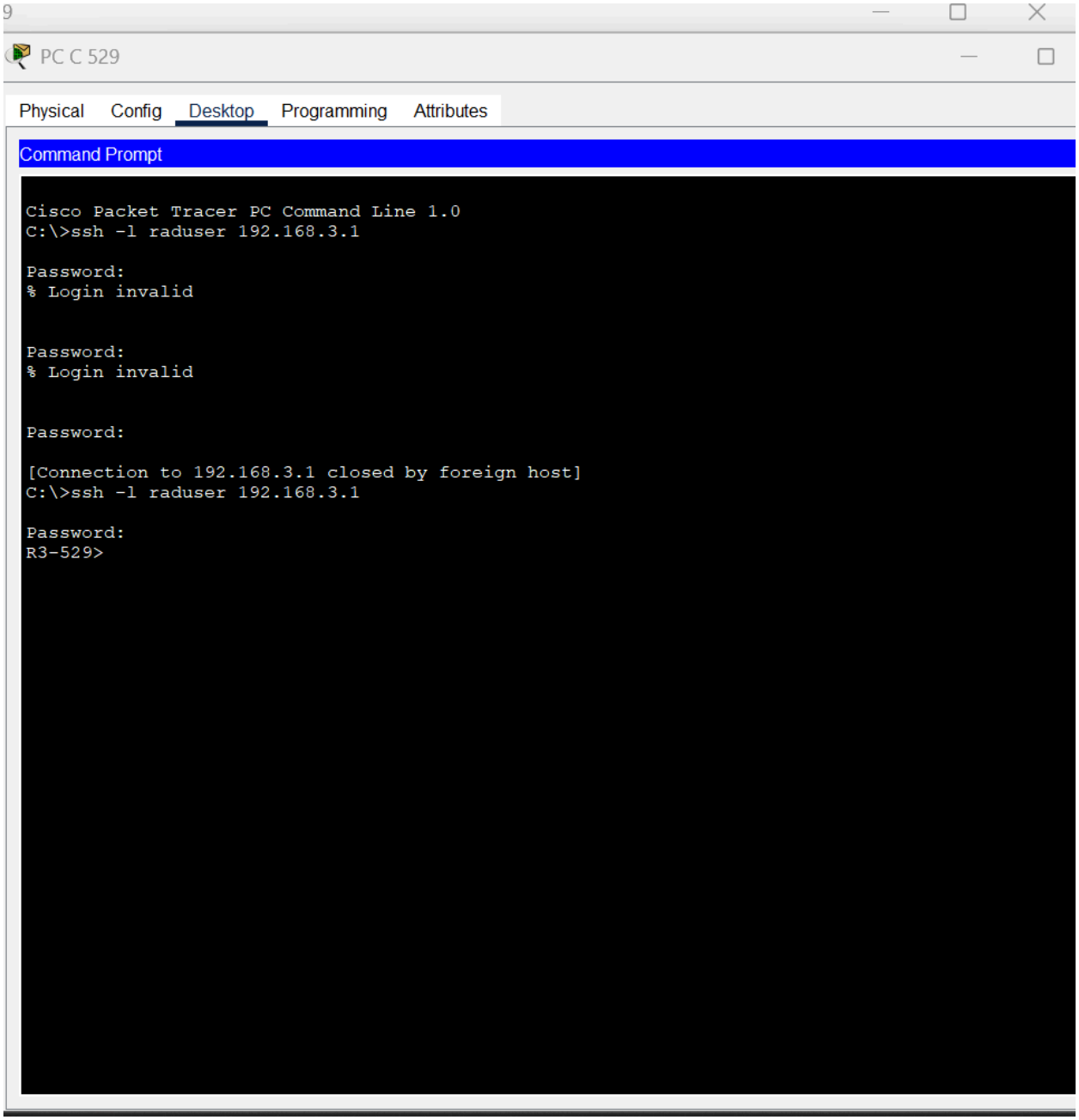

R2 529
Physical
Config
CLI
Attributes
IOS Command Line Interface
R2-529(config)#tacacs-server key tacacskey
R2-529(config)#aaa authentication login TAC-LOGIN group tacacs+ local
R2-529(config)#aaa authorization exec TAC-AUTH group tacacs+ local
R2-529(config)#line vty 0 4
R2-529(config-line)#login authentication TAC-LOGIN
R2-529(config-line)#authorization exec TAC-AUTh
^
% Invalid input detected at '^' marker.
R2-529(config-line)#authorization exec TAC-AUTH
^
% Invalid input detected at '^' marker.
R2-529(config-line)#transport input ssh
R2-529(config-line)#exit
R2-529(config)#end
R2-529#
%SYS-5-CONFIG_I: Configured from console by console
R2-529#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2-529(config)#hostname 529-R2
529-R2(config)#ip domain-name ccnasecurity.com
529-R2(config)#crypto key generate rsa
The name for the keys will be: 529-R2.ccnasecurity.com
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
529-R2(config)#ip ssh version 2
*Mar 1 1:23:12.296: %SSH-5-ENABLED: SSH 1.99 has been enabled
529-R2(config)#line vty 0 4
529-R2(config-line)#login authentication TAC-LOGIN
529-R2(config-line)#transport input ssh
529-R2(config-line)#exit
529-R2(config)#end
529-R2#
%SYS-5-CONFIG_I: Configured from console by console
529-R2#
Copy
Top


PC B 529
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Ping statistics for 192.168.3.3:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.3.3
Pinging 192.168.3.3 with 32 bytes of data:
Reply from 192.168.3.3: bytes=32 time=22ms TTL=126
Reply from 192.168.3.3: bytes=32 time=19ms TTL=126
Reply from 192.168.3.3: bytes=32 time=19ms TTL=126
Reply from 192.168.3.3: bytes=32 time=15ms TTL=126
Ping statistics for 192.168.3.3:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 15ms, Maximum = 22ms, Average = 18ms
C:\>ping 192.168.2.2
Pinging 192.168.2.2 with 32 bytes of data:
Reply from 192.168.2.2: bytes=32 time<1ms TTL=128
Reply from 192.168.2.2: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.2.2:
Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
C:\>ssh -l tacadmin 192.168.2.1
[Connection to 192.168.2.1 closed by foreign host]
C:\>ssh -l tacadmin 192.168.2.1
[Connection to 192.168.2.1 closed by foreign host]
C:\>ssh -l tacadmin 192.168.2.1
Password:
529-R2>
Top

Part 4: Configure Server-Based AAA Authentication Using RADIUS on R3.




Radius server 529
Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
AAA
Service
On
Off
Radius Port
1645
Network Configuration
Client Name
R3
Client IP
192.168.3.1
Secret
radiuskey
ServerType
Radius
Client Name
Client IP
Server Type
Key
1
R3
192.168.3.1
Radius
radiuskey
Add
Save
Remove
User Setup
Username
raduser
Password
radpa55
Username
Password
1
raduser
radpa55
Add
Save
Remove
Top


9
PC C 529
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l raduser 192.168.3.1
Password:
% Login invalid
Password:
% Login invalid
Password:
[Connection to 192.168.3.1 closed by foreign host]
C:\>ssh -l raduser 192.168.3.1
Password:
R3-529>