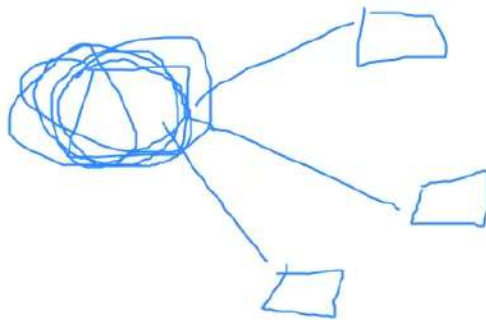
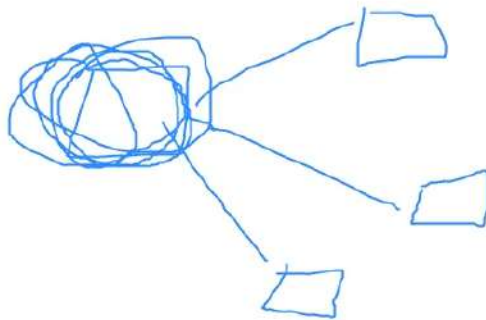


ACL (Access Control List)

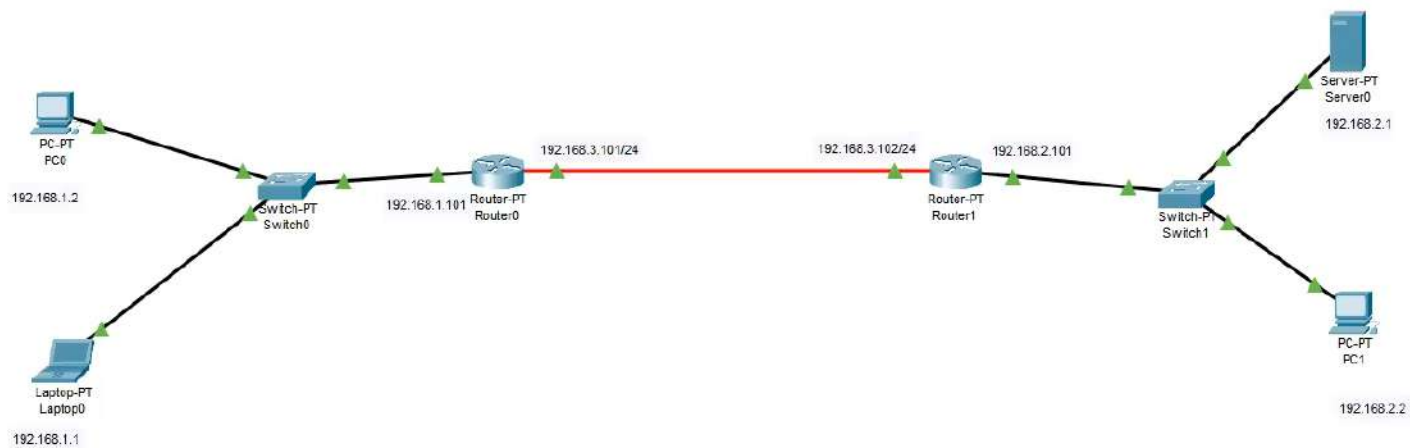


ACL (Access Control List)



I

Standard => 1-99 , 1300-1999, source IP address
Extended => 100-199, 2000-2699, IP, port, protocol



Time: 00:26:44

</

Configure Standard IPv4 ACLs

Numbered Standard IPv4 ACL Syntax

To create a numbered standard ACL, use the **access-list** command.

```
Router(config)# access-list access-list-number {deny | permit | remark text} source [source-wildcard] [log]
```

Parameter	Description
<i>access-list-number</i>	Number range is 1 to 99 or 1300 to 1999
deny	Denies access if the condition is matched
permit	Permits access if the condition is matched
remark text	(Optional) text entry for documentation purposes
<i>source</i>	Identifies the source network or host address to filter
<i>source-wildcard</i>	(Optional) 32-bit wildcard mask that is applied to the source
log	(Optional) Generates and sends an informational message when the ACE is matched

Note: Use the **no access-list** *access-list-number* global configuration command to remove a numbered standard ACL.

Configure Standard IPv4 ACLs

Numbered Standard IPv4 ACL Syntax

To create a numbered standard ACL, use the **access-list** command.

```
Router(config)# access-list access-list-number {deny | permit | remark text} source [source-wildcard] [log]
```

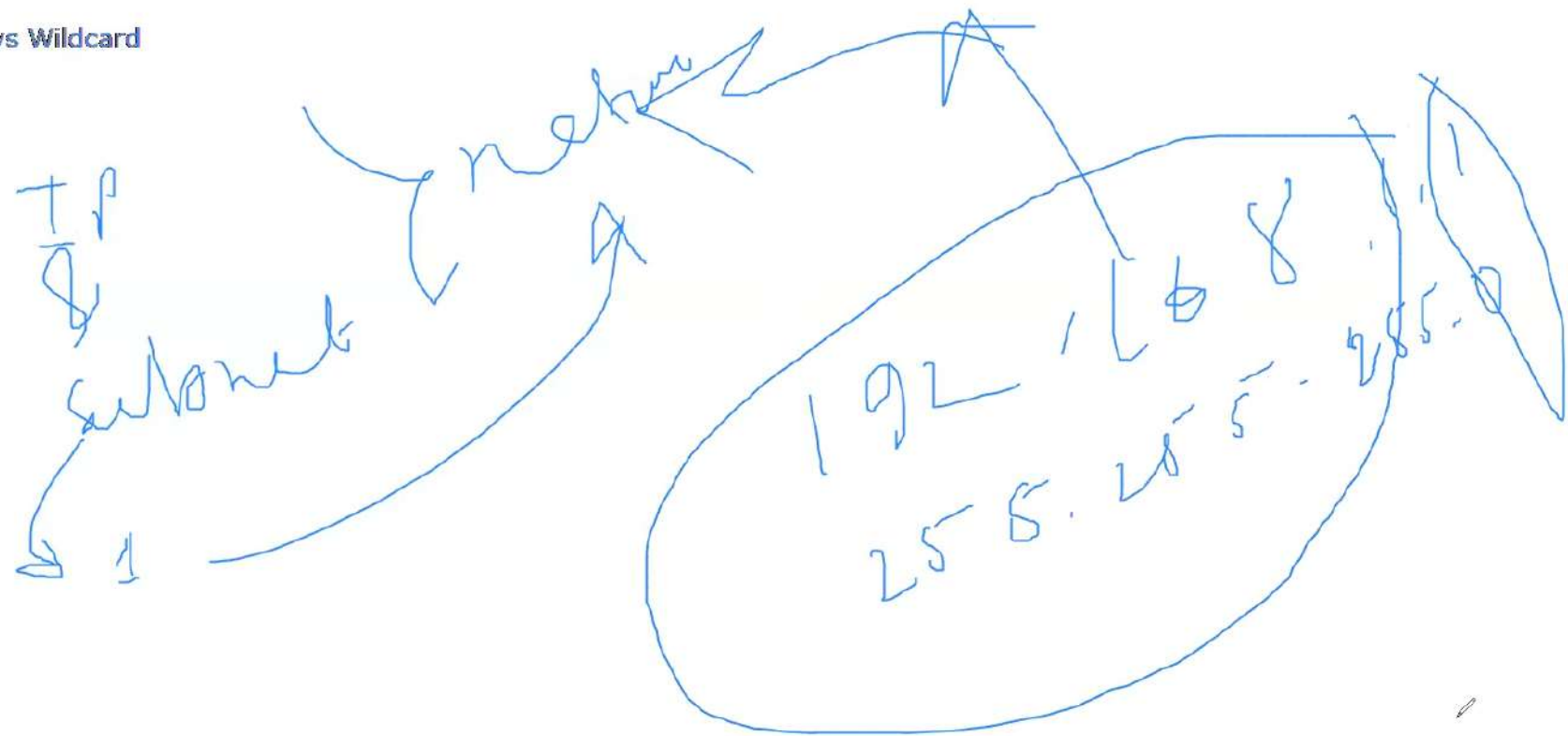
Parameter	Description
<i>access-list-number</i>	Number range is 1 to 99 or 1300 to 1999
deny	Denies access if the condition is matched
permit	Permits access if the condition is matched
remark text	(Optional) text entry for documentation purposes
<i>source</i>	Identifies the source network or host address to filter
<i>source-wildcard</i>	(Optional) 32-bit wildcard mask that is applied to the source
log	(Optional) Generates and sends an informational message when the ACE is matched

Note: Use the **no access-list access-list-number** global configuration command to remove a numbered standard ACL.

subnet

32
000
mark
1

Subnet Mask vs Wildcard



0 → take

1 → ignore

1 → subtract

0

Wildcard Masks in ACLs

Wildcard Mask Overview (Cont.)

Wildcard Mask	Last Octet (in Binary)	Meaning (0 - match, 1 - ignore)
0.0.0.0	00000000	Match all octets .
0.0.0.63	00111111	<ul style="list-style-type: none">• Match the first three octets• Match the two left most bits of the last octet• Ignore the last 6 bits
0.0.0.15	00001111	<ul style="list-style-type: none">• Match the first three octets• Match the four left most bits of the last octet• Ignore the last 4 bits of the last octet
0.0.0.248	11111100	<ul style="list-style-type: none">• Match the first three octets• Ignore the six left most bits of the last octet• Match the last two bits
0.0.0.255	11111111	<ul style="list-style-type: none">• Match the first three octet• Ignore the last octet

Router1

Physical Config CLI Attributes

IOS Command Line Interface

```
Router>
Router>en
Router#
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#access-list 10 remark for disable server
^
% Invalid input detected at '^' marker.

Router(config)#
Router(config)#access-list 10 remark for disable server
Router(config)#
Router(config)#
Router(config)#
Router(config)#access-list 10 deny 0.0.0.0 1.1.1.1
Router(config)#
Router(config)#
Router(config)#do show access-list
Standard IP access list 10
 10 deny 0.0.0.0 1.1.1.1
Router(config)#
```

Ctrl+FG to exit CLI focus

Copy Paste

☐ Top

Router1

Physical Config CLI Attributes

IOS Command Line Interface

```
Router>
Router>en
Router#
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#access-list 10 remark for disable server
^
% Invalid input detected at '^' marker.

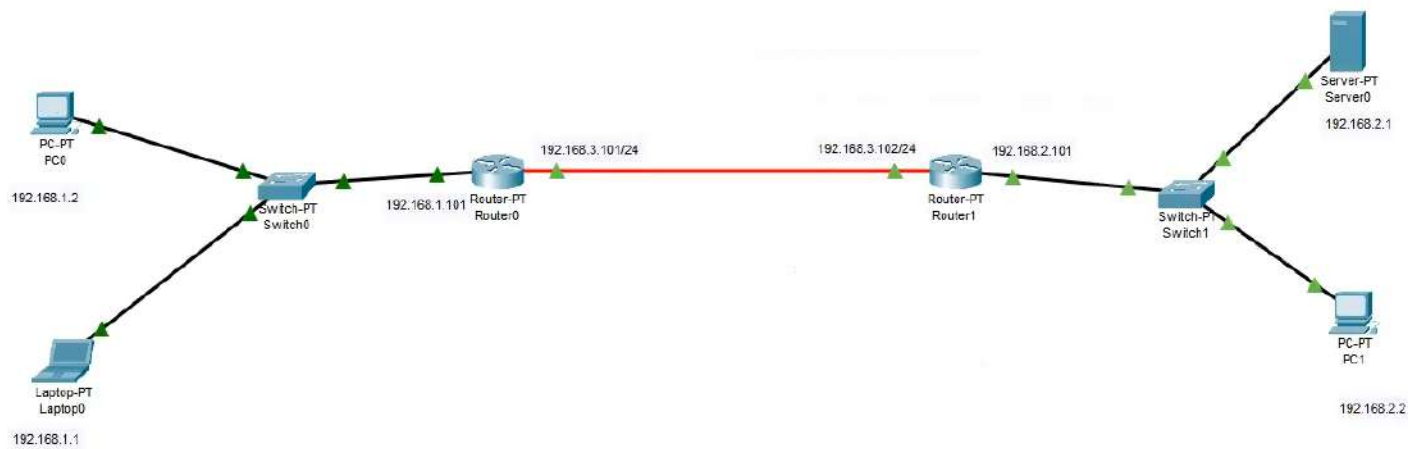
Router(config)#
Router(config)#access-list 10 remark for disable server
Router(config)#
Router(config)#
Router(config)#
Router(config)#access-list 10 deny 0.0.0.0 1.1.1.1
Router(config)#
Router(config)#do show access-list
Standard IP access list 10
  10 deny 0.0.0.0 1.1.1.1

Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#int fa0/0
Router(config-if)#
Router(config-if)#ip access-group 10 in
Router(config-if)#
Router(config-if)#
Router(config-if)#exit
Router(config)#
Router(config)#
```

Ctrl+FG to exit CLI focus

Copy Paste

☐ Top



Cisco Packet Tracer

File Edit Options View Tools Extensions Window Help

Logical

Physical

x: 1593 y: 599

Router

13:40:00

Event List

Simulation Panel

Time: 00:52:11.622

PLAY CONTROLS

Scenario 0

View

Delete

Toggle POV List Window

Fire

Last Status

Source

Destination

Type

Color

Time(sec)

Periodic

Num

Edit

Delete

Failed

PC0

Server0

ICMP

0.000

N

0

(edit)

(delete)

PC-PT PC0

192.168.1.2

Switch-PT Switch0

Laptop-PT Laptop0

192.168.1.1

Router-PT Router0

192.168.1.101

Router-PT Router1

192.168.3.102/24

192.168.2.101

Switch-PT Switch1

Server-PT Server0

192.168.2.1

PC-PT PC1

192.168.2.2

85°F

Haze

9:32 PM

6/21/2023

Simulation Panel

Event List

Vis.	Time(sec)	Last Device
	0.000	--
	0.001	PC0
	0.002	Switch0
	0.003	Router0
	0.004	Router1
	0.005	Switch1
	0.006	Server0
	0.007	Switch1
	0.008	Router1
Visible	0.009	Switch1

Reset Simulation

☒ Constant Delay

Captured to: 150.013 s

Play Controls

Event List Filters - Visible Events

ICMP

Edit Filters

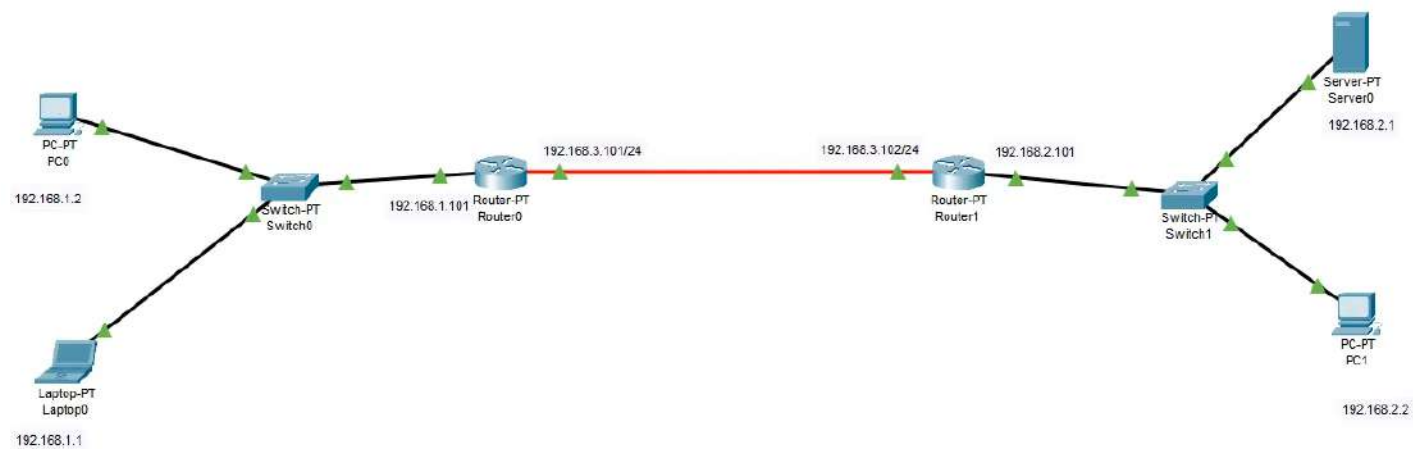
Show All/None

Event List

Realtime

Simulation

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Failed	PC0	Server0	ICMP		0.000	N	0	(edit)	(delete)



Router1

Physical Config CLI Attributes

IOS Command Line Interface

Press RETURN to get started.

```
Router>
Router>
Router>
Router>en
Router#
Router#
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#no access-list 10
Router(config)#
Router(config)#
Router(config)#
Router(config)#do show access-list
Router(config)#
Router(config)#
```

Ctrl+FG to exit CLI focus

Copy Paste

☐ Top

Configure Extended IPv4 ACLs

Apply a Numbered Extended IPv4 ACL

In this example, the ACL permits both HTTP and HTTPS traffic from the 192.168.10.0 network to go to any destination.

Extended ACLs can be applied in various locations. However, they are commonly applied close to the source. Here ACL 110 is applied inbound on the R1 G0/0/0 interface.

```
R1(config)# access-list 110 permit tcp 192.168.10.0 0.0.0.255 any eq www
R1(config)# access-list 110 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1(config)# interface g0/0/0
R1(config-if)# ip access-group 110 in
R1(config-if)# exit
R1(config)#
```

Router1

Physical Config CLI Attributes

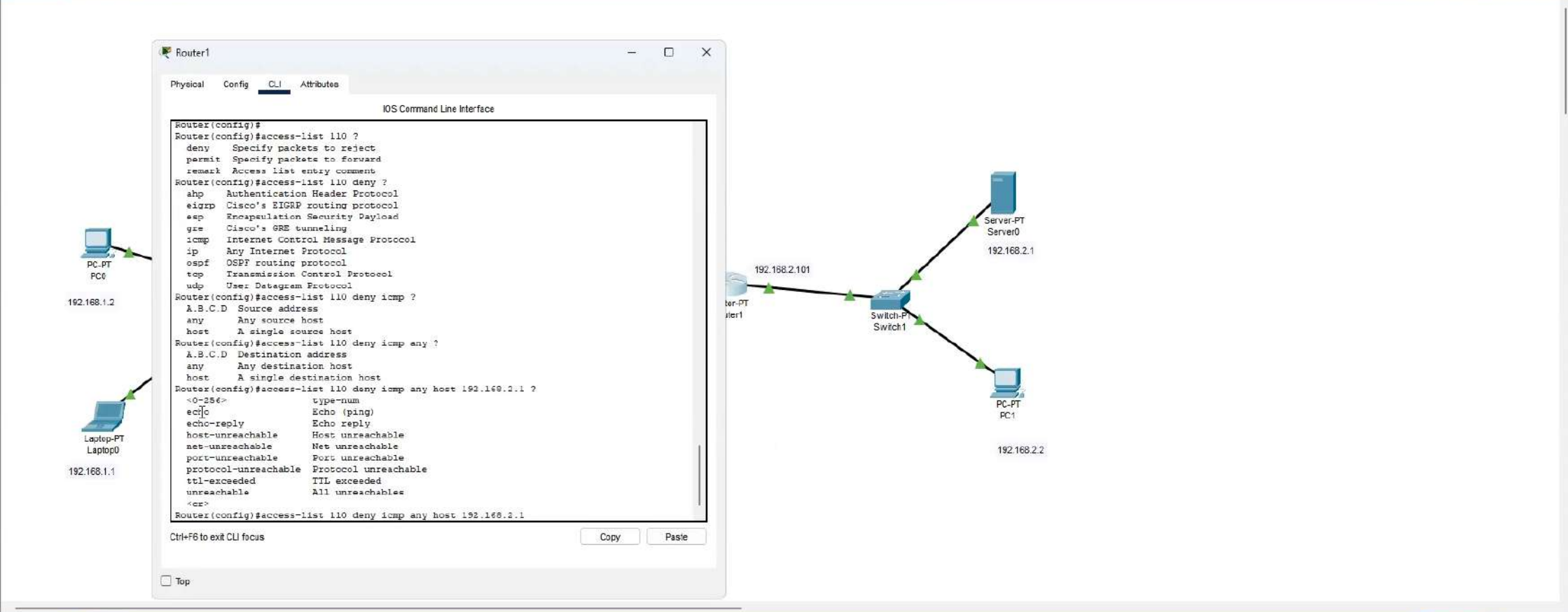
IOS Command Line Interface

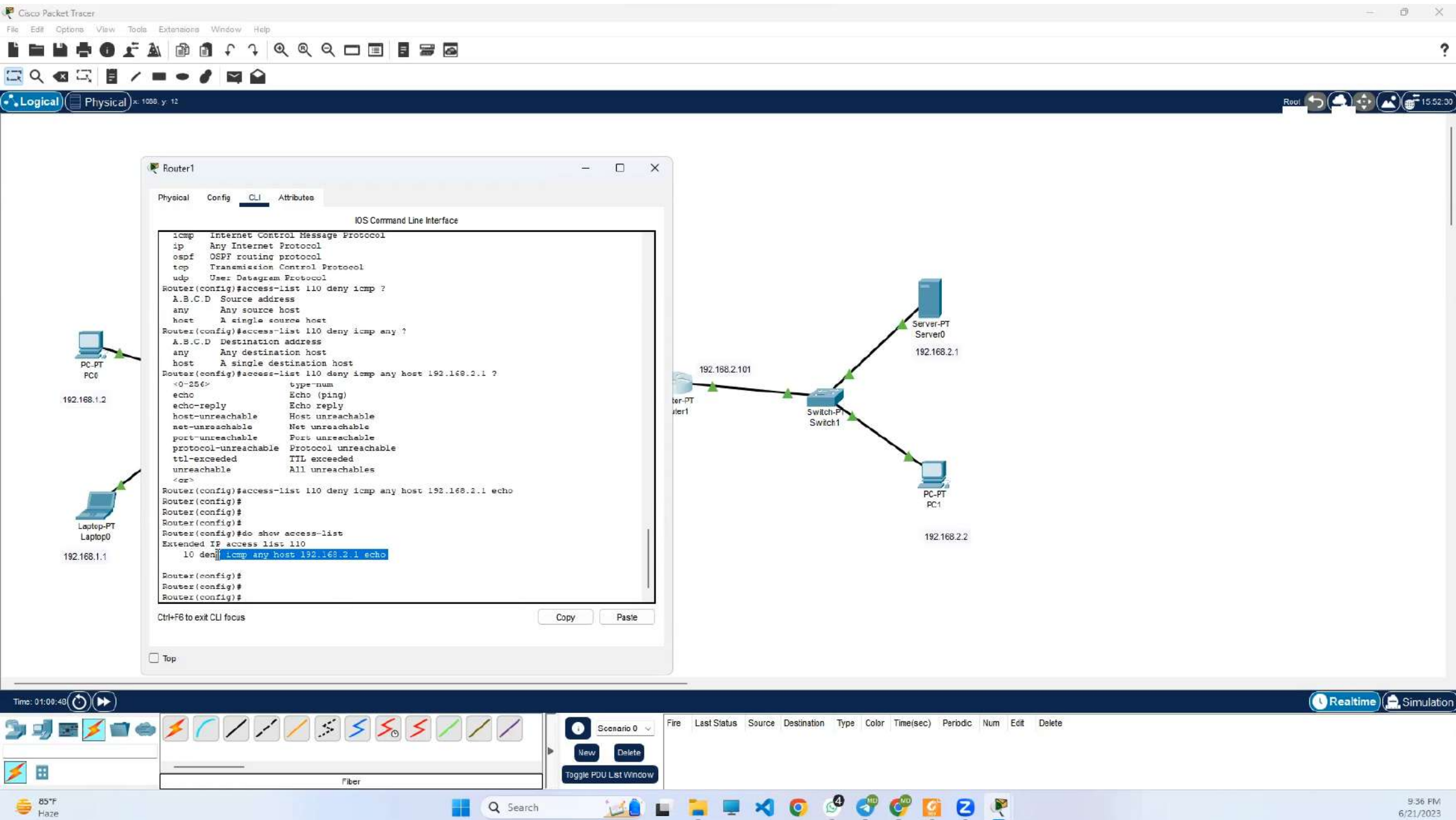
```
Router(config)#
Router(config)#access-list 110 ?
deny Specify packets to reject
permit Specify packets to forward
remark Access list entry comment
Router(config)#access-list 110 deny ?
ahp Authentication Header Protocol
eigrp Cisco's EIGRP routing protocol
esp Encapsulation Security Payload
gre Cisco's GRE tunneling
icmp Internet Control Message Protocol
ip Any Internet Protocol
ospf OSPF routing protocol
tcp Transmission Control Protocol
udp User Datagram Protocol
Router(config)#access-list 110 deny icmp ?
A.B.C.D Source address
any Any source host
host A single source host
Router(config)#access-list 110 deny icmp any ?
A.B.C.D Destination address
any Any destination host
host A single destination host
Router(config)#access-list 110 deny icmp any host 192.168.2.1 ?
<0-255> type-num
echo Echo (ping)
echo-reply Echo reply
host-unreachable Host unreachable
net-unreachable Net unreachable
port-unreachable Port unreachable
protocol-unreachable Protocol unreachable
ttl-exceeded TTL exceeded
unreachable All unreachable
<cr>
Router(config)#access-list 110 deny icmp any host 192.168.2.1
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top





Router1

Physical Config CLI Attributes

IOS Command Line Interface

```
Router(config)#access-list 110 deny icmp any ?
A.B.C.D Destination address
any Any destination host
host A single destination host
Router(config)#access-list 110 deny icmp any host 192.168.2.1 ?
<0-255> type-num
echo Echo (ping)
echo-reply Echo reply
host-unreachable Host unreachable
net-unreachable Net unreachable
port-unreachable Port unreachable
protocol-unreachable Protocol unreachable
ttl-exceeded TTL exceeded
unreachable All unreachables
<cr>
Router(config)#access-list 110 deny icmp any host 192.168.2.1 echo
Router(config)#
Router(config)#
Router(config)#
Router(config)#do show access-list
Extended IP access list 110
10 deny icmp any host 192.168.2.1 echo

Router(config)#
Router(config)#
Router(config)#int fa4/0
Router(config-if)#
Router(config-if)#ip access-group 110 in
Router(config-if)#
Router(config-if)#
Router(config-if)#exit
Router(config)#
Router(config)#
Router(config)#
```

Ctrl+FG to exit CLI focus

Copy Paste

Top

Cisco Packet Tracer

File Edit Options View Tools Extensions Window Help

Logical Physical x: 500, y: 549 Realtime 10:32:00

Router1

Physical Config CLI Attributes

IOS Command Line Interface

```
Router(config)#
Router(config)#do show access-list
Extended IP access list 110
  10 deny icmp any host 192.168.2.1 echo

Router(config)#
Router(config)#
Router(config)#int fa4/0
Router(config-if)#
Router(config-if)#ip access-group 110 in
Router(config-if)#
Router(config-if)#
Router(config-if)#exit
Router(config)#
Router(config)#
Router(config)#access-list 110 ?
deny Specify packets to reject
permit Specify packets to forward
remark Access list entry comment
Router(config)#access-list 110 permit ?
ahp Authentication Header Protocol
eigrp Cisco's EIGRP routing protocol
esp Encapsulation Security Payload
gre Cisco's GRE tunneling
icmp Internet Control Message Protocol
ip Any Internet Protocol
ospf OSPF routing protocol
tcp Transmission Control Protocol
udp User Datagram Protocol
Router(config)#access-list 110 permit icmp ?
A.B.C.D Source address
any Any source host
host A single source host
Router(config)#access-list 110 permit icmp
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

Time: 01:08:00

Realtime Simulation

Scenario 0

New Delete

Toggle POE List Window

Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete

85°F Haze

Search

9:41 PM 6/21/2023

Router1

Physical Config CLI Attributes

IOS Command Line Interface

```
Router(config)#
Router(config)#
Router(config)#access-list 110 ?
deny Specify packets to reject
permit Specify packets to forward
remark Access list entry comment
Router(config)#access-list 110 permit ?
ahp Authentication Header Protocol
eigrp Cisco's EIGRP routing protocol
esp Encapsulation Security Payload
gre Cisco's GRE tunneling
icmp Internet Control Message Protocol
ip Any Internet Protocol
ospf OSPF routing protocol
tcp Transmission Control Protocol
udp User Datagram Protocol
Router(config)#access-list 110 permit icmp ?
A.B.C.D Source address
any Any source host
host A single source host
Router(config)#access-list 110 permit icmp any
% Invalid input detected at '^' marker.
Router(config)#access-list 110 permit icmp any ?
A.B.C.D Destination address
any Any destination host
host A single destination host
Router(config)#access-list 110 permit icmp any any
Router(config)#do show access-list
Extended IP access list 110
10 deny icmp any host 192.168.2.1 echo (2 match(es))
20 permit icmp any any
Router(config)#
```

Ctrl+F8 to exit CLI focus

Copy Paste

☐ Top

Router1

Physical Config CLI Attributes

IOS Command Line Interface

```

remark Access list entry comment
Router(config)#access-list 110 permit ?
  ahp      Authentication Header Protocol
  eigrp    Cisco's EIGRP routing protocol
  esp      Encapsulation Security Payload
  gre      Cisco's GRE tunneling
  icmp     Internet Control Message Protocol
  ip       Any Internet Protocol
  ospf     OSPF routing protocol
  tcp      Transmission Control Protocol
  udp      User Datagram Protocol
Router(config)#access-list 110 permit icmp ?
  A.B.C.D  Source address
  any      Any source host
  host     A single source host
Router(config)#access-list 110 permit icmp any
% Invalid input detected at '^' marker.
Router(config)#access-list 110 permit icmp any ?
  A.B.C.D  Destination address
  any      Any destination host
  host     A single destination host
Router(config)#access-list 110 permit icmp any any
Router(config)#do show access-list
Extended IP access list 110
  10 deny icmp any host 192.168.2.1 echo (2 match(es))
  20 permit icmp any any
Router(config)#do show access-list
Extended IP access list 110
  10 deny icmp any host 192.168.2.1 echo (4 match(es))
  20 permit icmp any any (3 match(es))
Router(config)#no access-list
    
```

Ctrl+FG to exit CLI focus

Copy Paste

☐ Top

Router1

Physical Config CLI Attributes

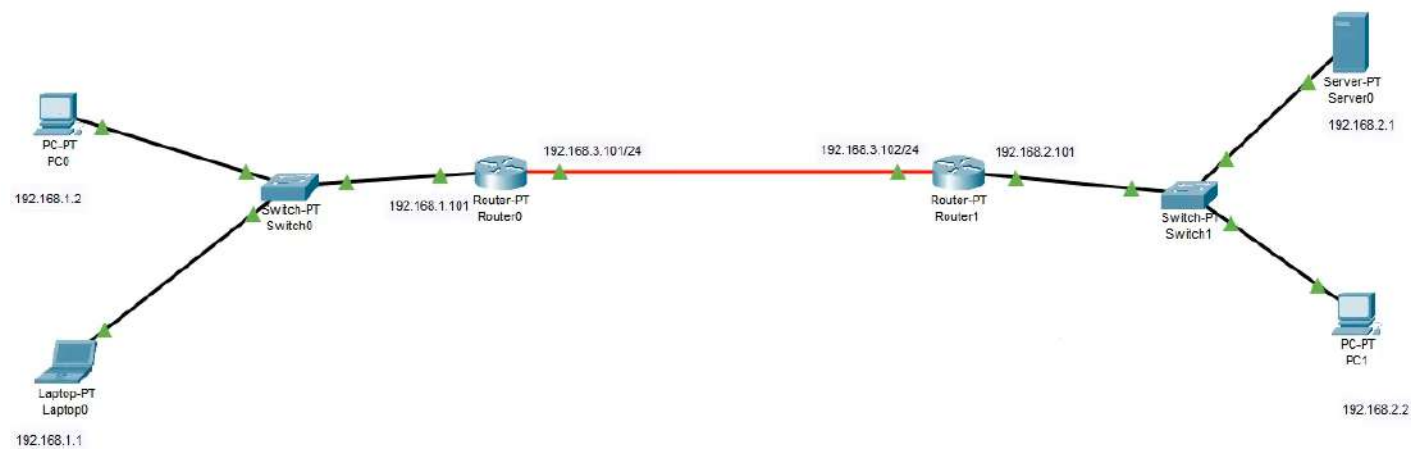
IOS Command Line Interface

```
esp Encapsulation Security Payload
gre Cisco's GRE tunneling
icmp Internet Control Message Protocol
ip Any Internet Protocol
ospf OSPF routing protocol
tcp Transmission Control Protocol
udp User Datagram Protocol
Router(config)#access-list 110 permit icmp ?
A.B.C.D Source address
any Any source host
host A single source host
Router(config)#access-list 110 permit icmp any
% Invalid input detected at '^' marker.
Router(config)#access-list 110 permit icmp any ?
A.B.C.D Destination address
any Any destination host
host A single destination host
Router(config)#access-list 110 permit icmp any any
Router(config)#do show access-list
Extended IP access list 110
 10 deny icmp any host 192.168.2.1 echo (2 match(es))
 20 permit icmp any any
Router(config)#do show access-list
Extended IP access list 110
 10 deny icmp any host 192.168.2.1 echo (4 match(es))
 20 permit icmp any any (3 match(es))
Router(config)#no access-list 110
Router(config)#access-list 110 permit icmp any any
Router(config)#
Router(config)#
Router(config)#
```

Ctrl+FG to exit CLI focus

Copy Paste

Top



Cisco Packet Tracer

File Edit Options View Tools Extensions Window Help

Logical Physical x: 1318 y: 51

Router1

Physical Config CLI Attributes

IOS Command Line Interface

```
any Any source host
host A single source host
Router(config)#access-list 110 permit icmp any
^
% Invalid input detected at '^' marker.

Router(config)#access-list 110 permit icmp any ?
A.B.C.D Destination address
any Any destination host
host A single destination host
Router(config)#access-list 110 permit icmp any any
Router(config)#do show access-list
Extended IP access list 110
  10 deny icmp any host 192.168.2.1 echo (2 match(es))
  20 permit icmp any any
Router(config)#do show access-list
Extended IP access list 110
  10 deny icmp any host 192.168.2.1 echo (4 match(es))
  20 permit icmp any any (3 match(es))

Router(config)#no access-list 110
Router(config)#access-list 110 permit icmp any any
Router(config)#
Router(config)#
Router(config)#access-list 110 deny icmp any host 192.168.2.1 echo
Router(config)#
Router(config)#
Router(config)#int fa4/0
Router(config-if)#
Router(config-if)#ip access-group 110 in
Router(config-if)#
Router(config-if)#exit
Router(config)#
Router(config)#
```

Ctrl+FG to exit CLI focus

Copy Paste

Time: 01:23:54

85°F Haze

Scenario 0

New Delete

Toggle POE List Window

Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete

9:48 PM 6/21/2023

Router1

Physical Config CLI Attributes

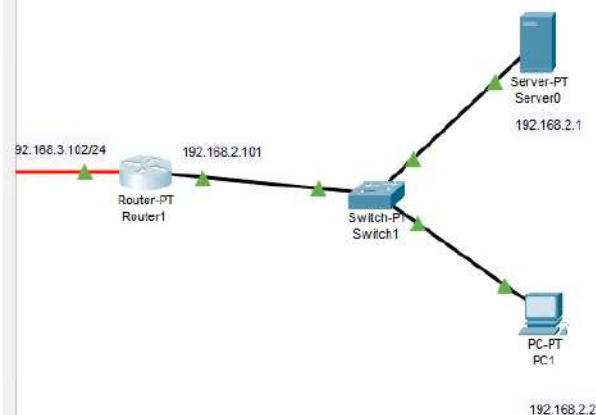
IOS Command Line Interface

```
Router(config)#access-list 110 deny icmp any host 192.168.2.1 echo
Router(config)#
Router(config)#
Router(config)#int fa4/0
Router(config-if)#
Router(config-if)#ip access-group 110 in
Router(config-if)#
Router(config-if)#exit
Router(config)#
Router(config)#no access-list 110
Router(config)#
Router(config)#access-list 110 permit icmp any host 192.168.2.2 ?
<0-255>      type-num
echo          Echo (ping)
echo-reply    Echo reply
host-unreachable Host unreachable
net-unreachable Net unreachable
port-unreachable Port unreachable
protocol-unreachable Protocol unreachable
ttl-exceeded  TTL exceeded
unreachable   All unreachables
<cr>
Router(config)#access-list 110 deny icmp any host 192.168.2.1 echo
Router(config)#access-list 110 deny icmp any host 192.168.2.1 echo-reply
Router(config)#access-list 110 permit icmp any host 192.168.2.2 echo
Router(config)#access-list 110 permit icmp any host 192.168.2.2 echo-reply
Router(config)#do show access-list
Extended IP access list 110
 10 deny icmp any host 192.168.2.1 echo
 20 deny icmp any host 192.168.2.1 echo-reply
 30 permit icmp any host 192.168.2.2 echo
 40 permit icmp any host 192.168.2.2 echo-reply
Router(config)#
Router(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top



Router1

Physical Config CLI Attributes

IOS Command Line Interface

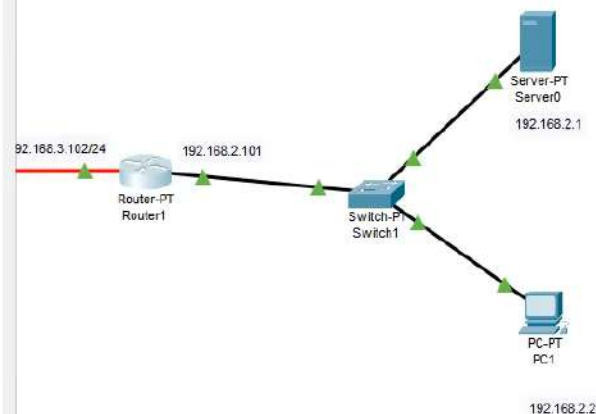
```
Router(config)#
Router(config)#no access-list 110
Router(config)#
Router(config)#access-list 110 permit icmp any host 192.168.2.2 ?
<0-255>          type-num
echo              Echo (ping)
echo-reply        Echo reply
host-unreachable  Host unreachable
net-unreachable   Net unreachable
port-unreachable  Port unreachable
protocol-unreachable Protocol unreachable
ttl-exceeded      TTL exceeded
unreachable       All unreachables
<cr>
Router(config)#access-list 110 deny icmp any host 192.168.2.1 echo
Router(config)#access-list 110 deny icmp any host 192.168.2.1 echo-reply
Router(config)#access-list 110 permit icmp any host 192.168.2.2 echo
Router(config)#access-list 110 permit icmp any host 192.168.2.2 echo-reply
Router(config)#do show access-list
Extended IP access list 110
 10 deny icmp any host 192.168.2.1 echo
 20 deny icmp any host 192.168.2.1 echo-reply
 30 permit icmp any host 192.168.2.2 echo
 40 permit icmp any host 192.168.2.2 echo-reply

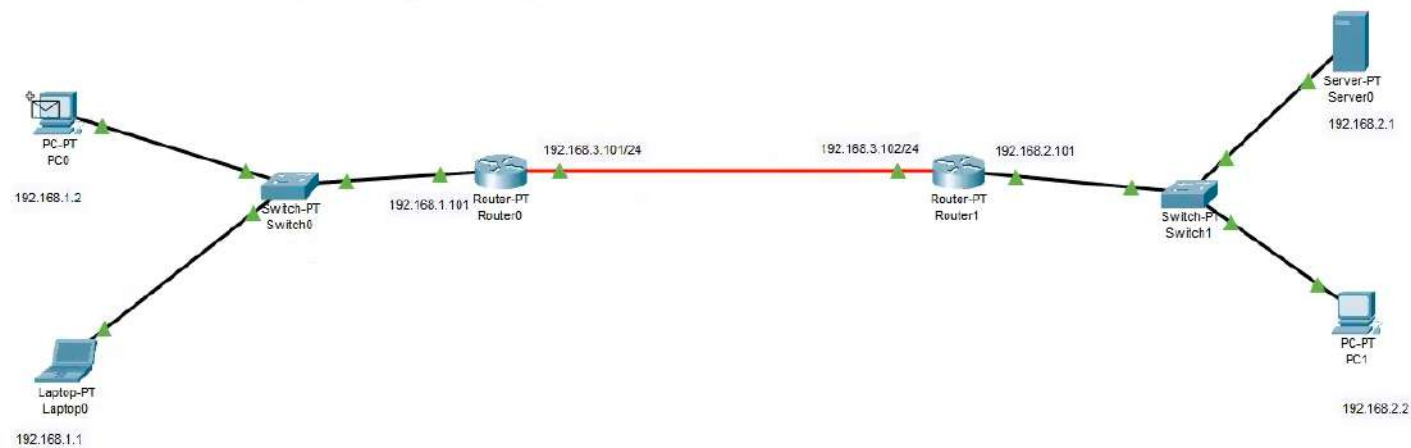
Router(config)#
Router(config)#int fa4/0
Router(config-if)#
Router(config-if)#ip access-group 110 in
Router(config-if)#
Router(config-if)#exit
Router(config)#
Router(config)#
Router(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top





Router1

Physical Config CLI Attributes

IOS Command Line Interface

```

Host-unreachable      Host unreachable
net-unreachable       Net unreachable
port-unreachable      Port unreachable
protocol-unreachable  Protocol unreachable
ttl-exceeded          TTL exceeded
unreachable           All unreachables
<cr>
Router(config)#access-list 110 deny icmp any host 192.168.2.1 echo
Router(config)#access-list 110 deny icmp any host 192.168.2.1 echo-reply
Router(config)#access-list 110 permit icmp any host 192.168.2.2 echo
Router(config)#access-list 110 permit icmp any host 192.168.2.2 echo-reply
Router(config)#do show access-list
Extended IP access list 110
 10 deny icmp any host 192.168.2.1 echo
 20 deny icmp any host 192.168.2.1 echo-reply
 30 permit icmp any host 192.168.2.2 echo
 40 permit icmp any host 192.168.2.2 echo-reply

Router(config)#
Router(config)#int fa4/0
Router(config-if)#
Router(config-if)#ip access-group 110 in
Router(config-if)#
Router(config-if)#exit
Router(config)#
Router(config)#do show access-list
Extended IP access list 110
 10 deny icmp any host 192.168.2.1 echo (3 match(es))
 20 deny icmp any host 192.168.2.1 echo-reply
 30 permit icmp any host 192.168.2.2 echo (1 match(es))
 40 permit icmp any host 192.168.2.2 echo-reply

Router(config)#
    
```

Ctrl+FG to exit CLI focus

Copy Paste

☐ Top