ISAA LAB ASSIGNMENT - 2

NAME	APOORVA REDDY BAGEPALLI
REGISTRATION NUMBER	19BCE2196

Intrusion Detection System

- Two PCs and a server is connected to switches respectively
- Three routers are connected with one of the router being an intermediate
- Copper straight through wire is used to connect with PCs, server and switches
- Serial DTE is used to connect between routers
- IP addresses are configured in devices
- Default gateway is configured in the routers
- Intrusion detection is implemented in middle router command line

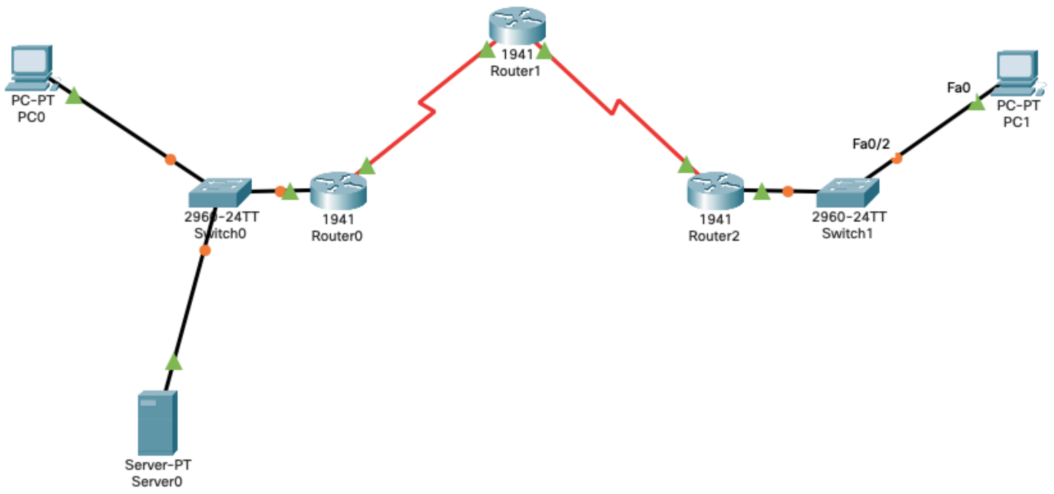
CODES

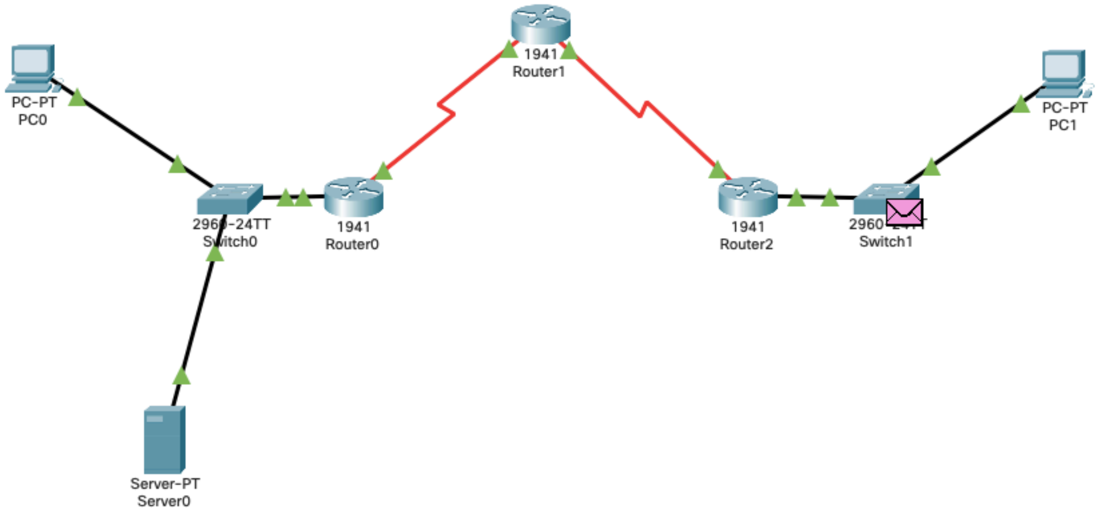
```
Router#show version
Router#configure terminal
Router(config)#license boot module c1900 technology-package securityk9
Router(config)#exit
Router#reload
Router>enable
Router#show version
Router#clock set 09:50:00 24 August 2021
Router#mkdir flash
Router#configure terminal
Router(config)#ip ips config location flash:flash
Router(config)#ip ips name iosips
Router(config)#ip ips notify log
Router(config)#ip ips signature-c
Router(config-ips-category)#ip ips signature-category
Router(config-ips-category)#category all
Router(config-ips-category-action)#retired true
Router(config-ips-category-action)#exit
Router(config-ips-category)#category ios_ips basic
Router(config-ips-category-action)#retired false
Router(config-ips-category-action)#exit
Router(config-ips-category)#exit
Router(config)#interface serial 0/1/0
Router(config-if)#ip ips iosips out
Router(config-if)#exit
```

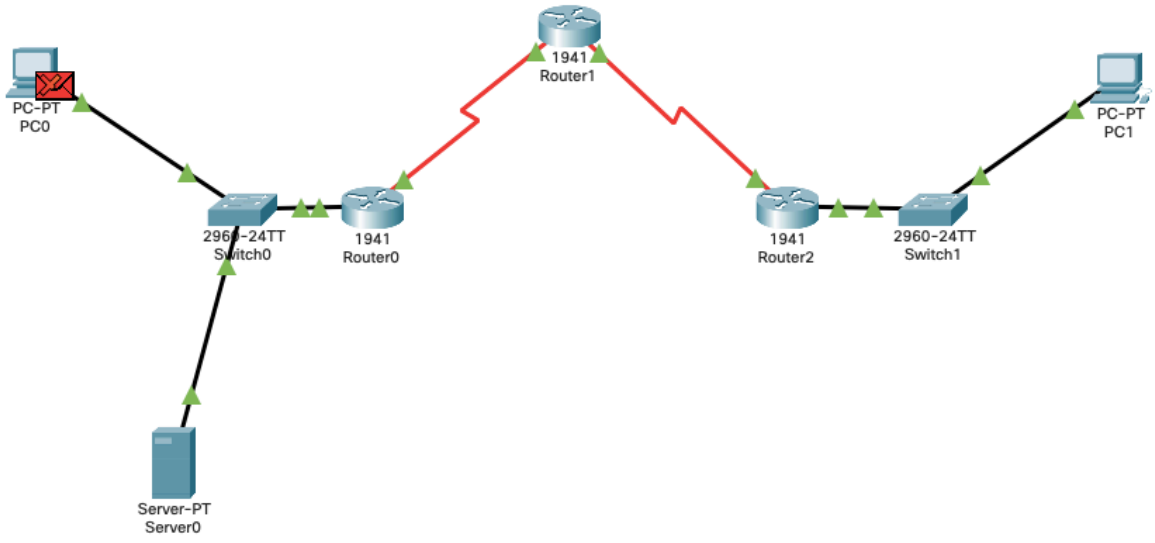
Part 2. Modify the signature

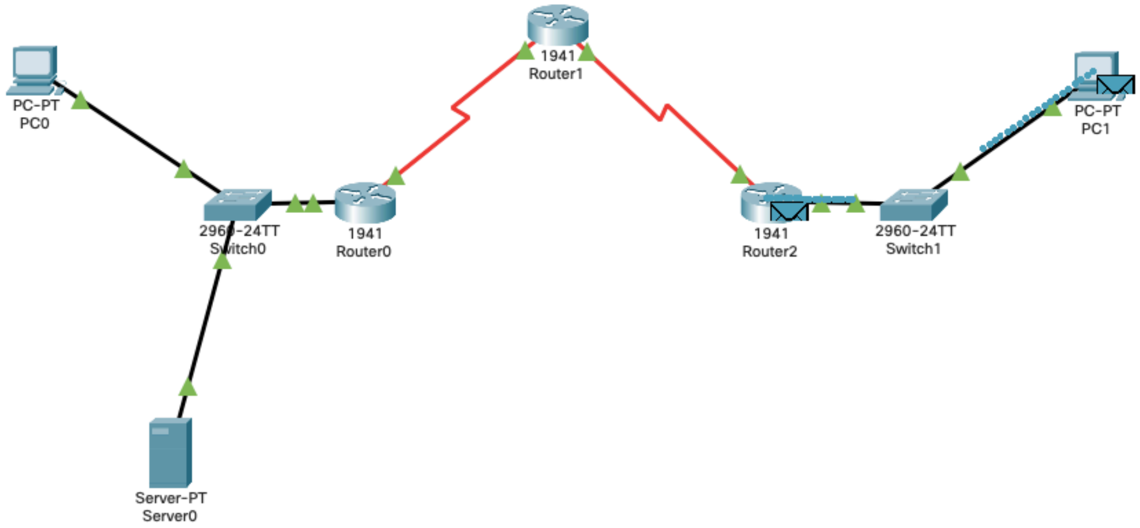
```
Router(config)#ip ips signature-d
Router(config-sigdef)#ip ips signature-definition
Router(config-sigdef)#signature 2004 0
Router(config-sigdef-sig)#status
Router(config-sigdef-sig-status)#retired false
Router(config-sigdef-sig-status)#enabled true
Router(config-sigdef-sig-status)#exit
Router(config-sigdef-sig)#engine
Router(config-sigdef-sig-engine)#event-action prod
Router(config-sigdef-sig-engine)#event-action produce-alert
Router(config-sigdef-sig-engine)#event-action deny
Router(config-sigdef-sig-engine)#event-action deny-packet-inline
Router(config-sigdef-sig-engine)#exit
Router(config-sigdef-sig)#exit
Router(config-sigdef)#exit
```

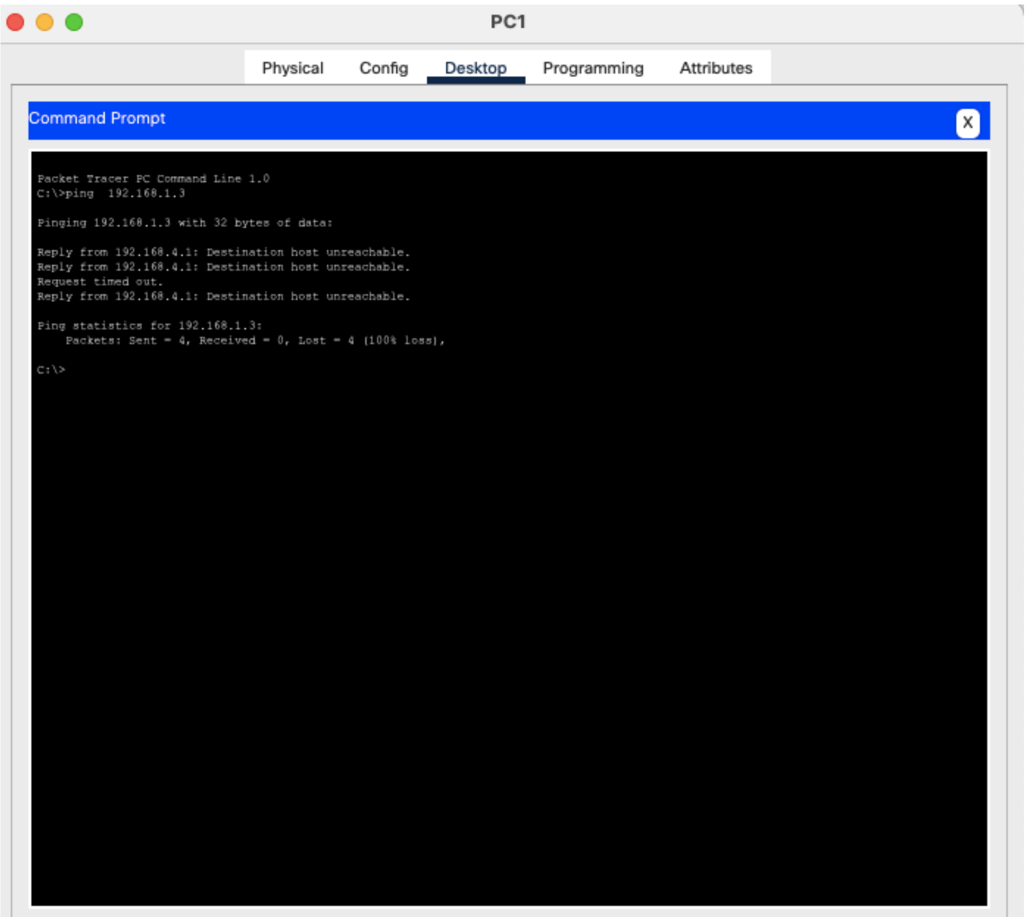
SCREENSHOTS



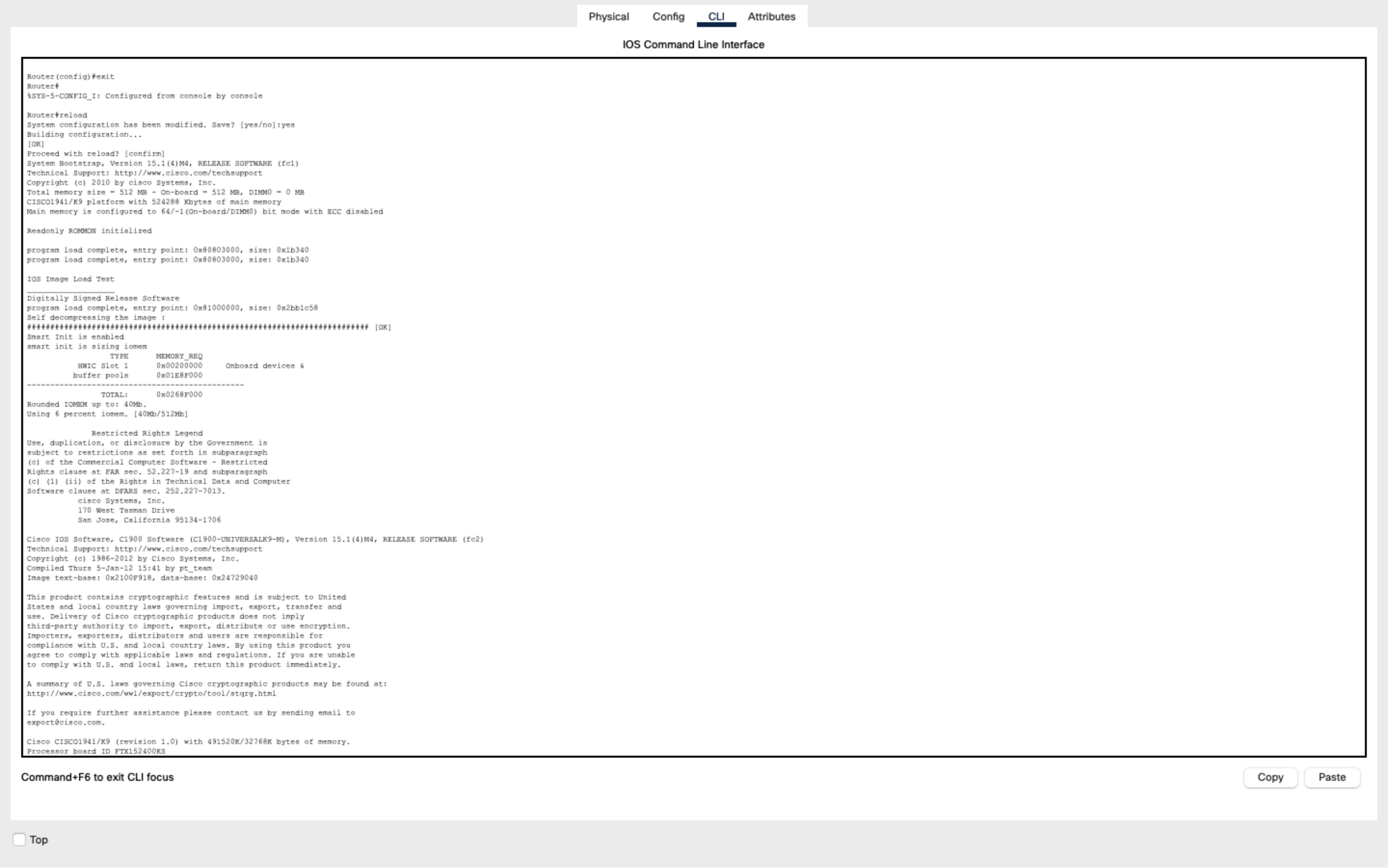




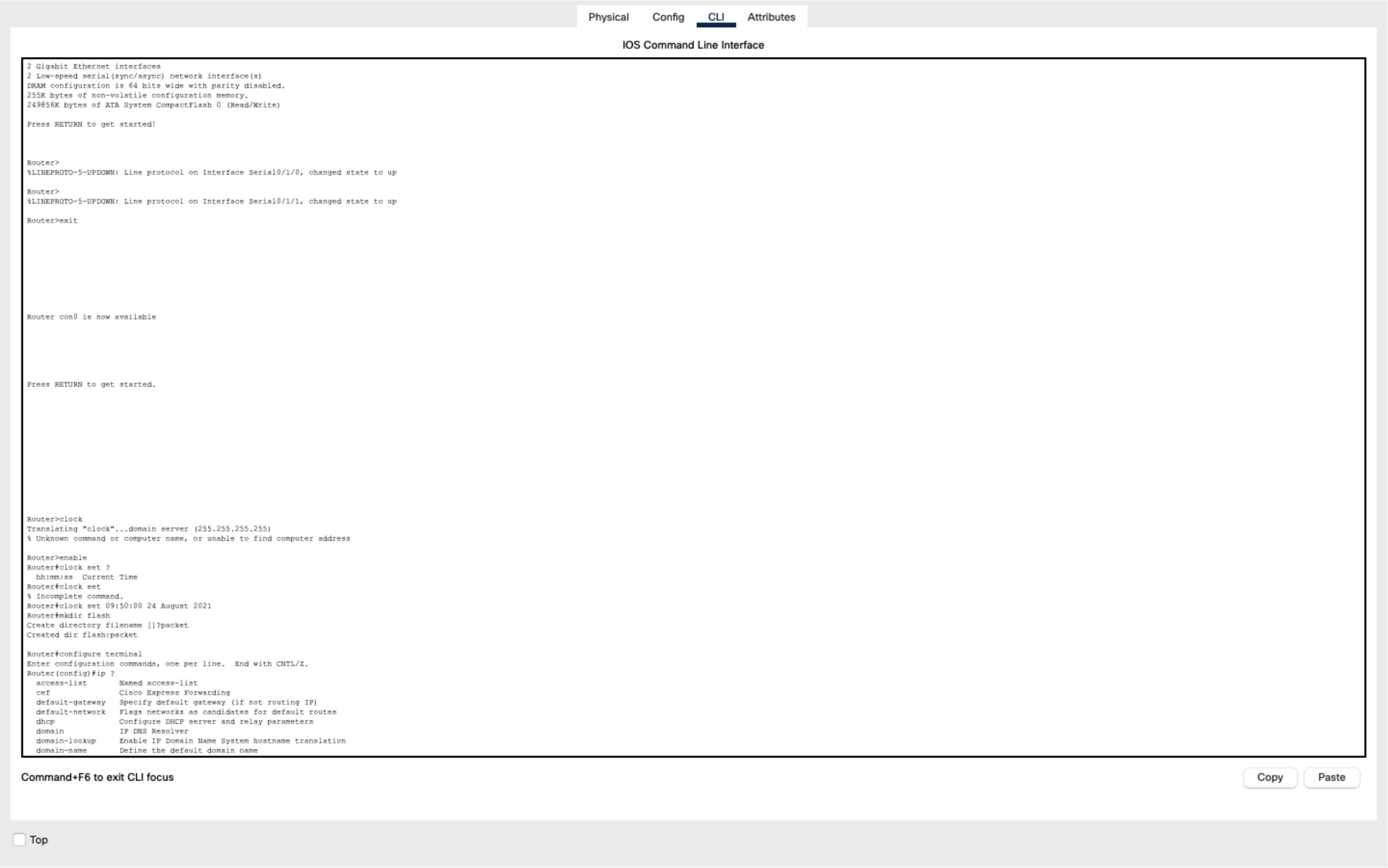




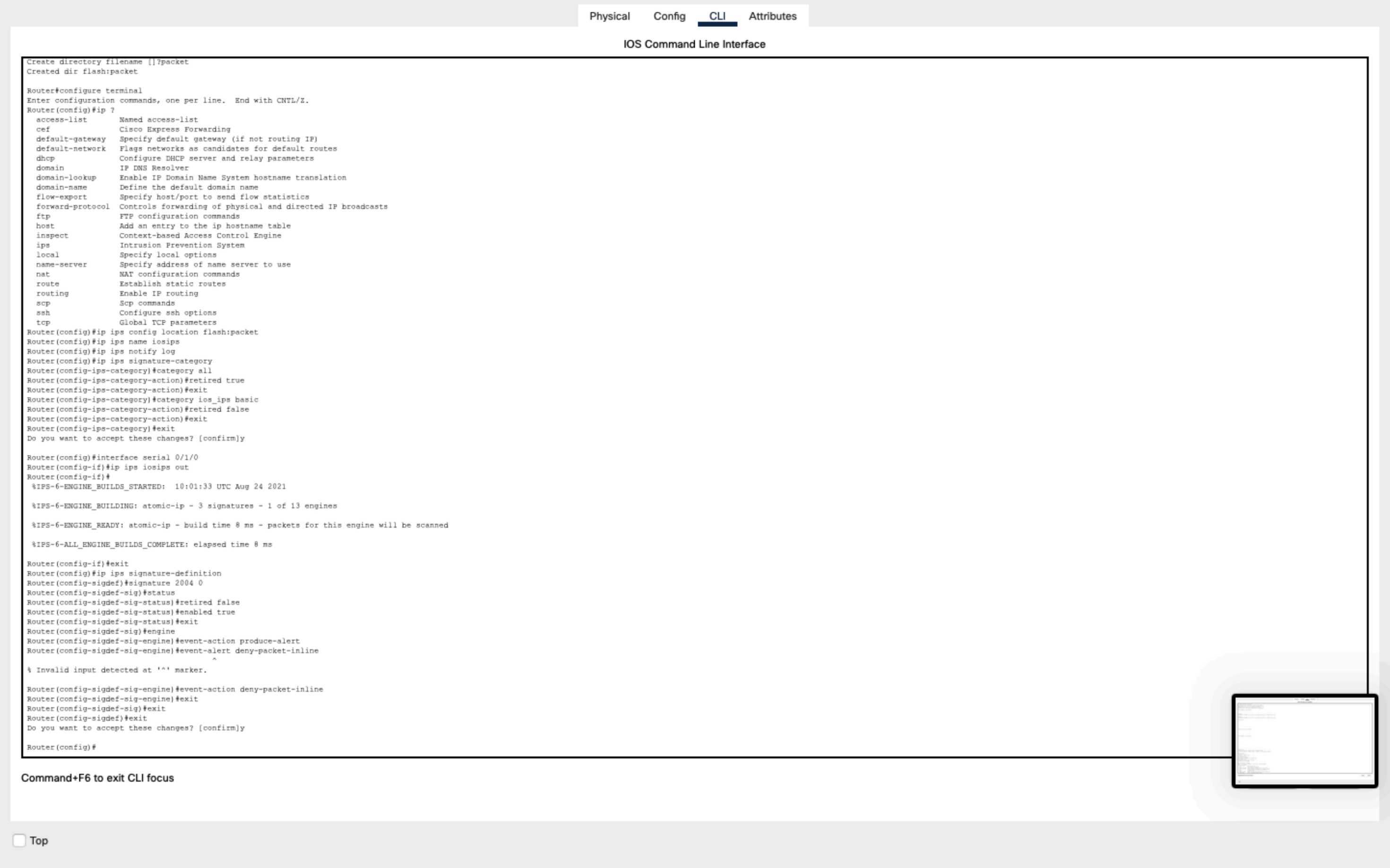
```
Packet Tracer PC Command Line 1.0
C:\>ping  192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.4.1: Destination host unreachable.
Reply from 192.168.4.1: Destination host unreachable.
Request timed out.
Reply from 192.168.4.1: Destination host unreachable.

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```



```
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#reload
System configuration has been modified. Save? [yes/no]:yes
Building configuration...
[OK]
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC disabled

Readonly ROMMON initialized

program load complete, entry point: 0x80803000, size: 0x1b340
program load complete, entry point: 0x80803000, size: 0x1b340

IOS Image Load Test
___________________
Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x2bb1c58
Self decompressing the image :
########################################################################## [OK]
Smart Init is enabled
smart init is sizing iomem
                  TYPE      MEMORY_REQ
           HWIC Slot 1      0x00200000     Onboard devices &
          buffer pools      0x01E8F000
------------------------------------------------
                TOTAL:      0x0268F000
Rounded IOMEM up to: 40Mb.
Using 6 percent iomem. [40Mb/512Mb]

              Restricted Rights Legend
Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
           cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706

Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thurs 5-Jan-12 15:41 by pt_team
Image text-base: 0x2100F918, data-base: 0x24729040

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

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!



Router>
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up

Router>
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/1, changed state to up

Router>exit









Router con0 is now available






Press RETURN to get started.














Router>clock
Translating "clock"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address

Router>enable
Router#clock set ?
  hh:mm:ss  Current Time
Router#clock set
% Incomplete command.
Router#clock set 09:50:00 24 August 2021
Router#mkdir flash
Create directory filename []?packet
Created dir flash:packet

Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip ?
  access-list       Named access-list
  cef               Cisco Express Forwarding
  default-gateway   Specify default gateway (if not routing IP)
  default-network   Flags networks as candidates for default routes
  dhcp              Configure DHCP server and relay parameters
  domain            IP DNS Resolver
  domain-lookup     Enable IP Domain Name System hostname translation
  domain-name       Define the default domain name
```



```
Create directory filename []?packet
Created dir flash:packet

Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip ?
  access-list       Named access-list
  cef               Cisco Express Forwarding
  default-gateway   Specify default gateway (if not routing IP)
  default-network   Flags networks as candidates for default routes
  dhcp              Configure DHCP server and relay parameters
  domain            IP DNS Resolver
  domain-lookup     Enable IP Domain Name System hostname translation
  domain-name       Define the default domain name
  flow-export       Specify host/port to send flow statistics
  forward-protocol  Controls forwarding of physical and directed IP broadcasts
  ftp               FTP configuration commands
  host              Add an entry to the ip hostname table
  inspect           Context-based Access Control Engine
  ips               Intrusion Prevention System
  local             Specify local options
  name-server       Specify address of name server to use
  nat               NAT configuration commands
  route             Establish static routes
  routing           Enable IP routing
  scp               Scp commands
  ssh               Configure ssh options
  tcp               Global TCP parameters
Router(config)#ip ips config location flash:packet
Router(config)#ip ips name iosips
Router(config)#ip ips notify log
Router(config)#ip ips signature-category
Router(config-ips-category)#category all
Router(config-ips-category-action)#retired true
Router(config-ips-category-action)#exit
Router(config-ips-category)#category ios_ips basic
Router(config-ips-category-action)#retired false
Router(config-ips-category-action)#exit
Router(config-ips-category)#exit
Do you want to accept these changes? [confirm]y

Router(config)#interface serial 0/1/0
Router(config-if)#ip ips iosips out
Router(config-if)#
 %IPS-6-ENGINE_BUILDS_STARTED:  10:01:33 UTC Aug 24 2021

 %IPS-6-ENGINE_BUILDING: atomic-ip - 3 signatures - 1 of 13 engines

 %IPS-6-ENGINE_READY: atomic-ip - build time 8 ms - packets for this engine will be scanned

 %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 8 ms

Router(config-if)#exit
Router(config)#ip ips signature-definition
Router(config-sigdef)#signature 2004 0
Router(config-sigdef-sig)#status
Router(config-sigdef-sig-status)#retired false
Router(config-sigdef-sig-status)#enabled true
Router(config-sigdef-sig-status)#exit
Router(config-sigdef-sig)#engine
Router(config-sigdef-sig-engine)#event-action produce-alert
Router(config-sigdef-sig-engine)#event-alert deny-packet-inline
                                       ^
% Invalid input detected at '^' marker.

Router(config-sigdef-sig-engine)#event-action deny-packet-inline
Router(config-sigdef-sig-engine)#exit
Router(config-sigdef-sig)#exit
Router(config-sigdef)#exit
Do you want to accept these changes? [confirm]y

Router(config)#
```

Command+F6 to exit CLI focus

□ Top