

CSIT Department

Bhaktapur Multiple Campus

Doodhpati, Bhaktapur



Lab sheet -7

A LAB REPORT OF

Computer Networks (CSC258)

Submitted By:

Samir Deshar

Roll No:70

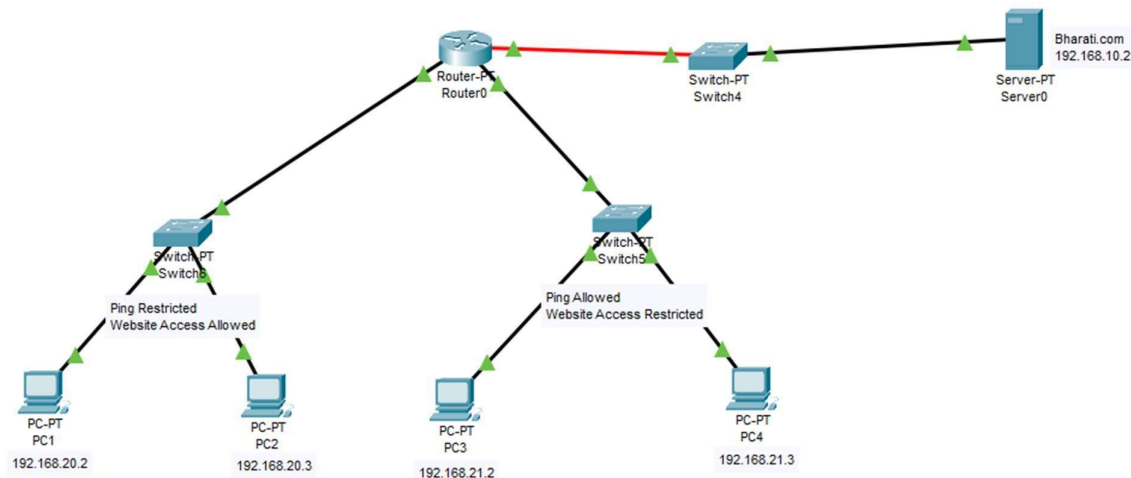
Submitted To

Ramesh Kharbuja

OBJECTIVES:

1. To block echo request (“ping”) but allow https request in one network and vice-versa in another network using Access Control List (ACL).

Network Configuration



Theory

- Access Control List (ACL)

Access Control Lists (ACLs) is a set of rules that provides a condition, either to permit or deny the network traffic. The major purpose of ACL is to filter and identify traffic.

Access lists are applied on either inbound (packets received on interface before routing) or outbound (packets leaving an interface after routing).

While filtering the traffic, access lists are implemented on interfaces. Only one access list per interface, per protocol, per direction is allowed.

- Types of Access Lists

- o Standard

Numbered Access List are broken down into several ranges, each dedicated to specific protocol. It has number range from 1-99 and 1300-1999. It specifies deny/permit traffic from only the source address with optional wildcard mask for filtering subnet range. There is by default deny all clause as the last statement with any ACL so we need to add permit any as a last statement to deny a specific IP.

It should be placed closest to the destination network. It is based upon source IP only.

Syntax:

Router(config)#access-list [1-99] [permit/deny] [source address] [wildcard mask][log]

- o Extended Numbered Access List

Extended access lists are based upon source IP, destination IP, protocol, and port number. The number range is from 100-199 and 2000-2699. It provides us additional feature to permit or deny a specific IP, TCP or UDP application-based protocol. It should be placed closest to the source network.

Syntax:

```
Router(config)#access-list [100-199] [permit/deny] [protocol] [source address]  
[wildcard mask] [destination address] [wildcard mask ] [operator[port]] [log]
```

o Standard Named Access List

Named ACL is configured with a name instead of a number. It has the same rules as a standard numbered ACL. Named ACL provides a bit more flexibility. Descriptive names can be used instead of numbers. And additionally, individual lines can be removed from named ACL which isn't possible in numbered ACL. Syntax:

```
Router(config)#access-list [name] [permit/deny] [source address] [wildcard  
mask][log]
```

o Extended Named Access List

It has the same rules as a standard numbered ACL except the use of name instead of number.

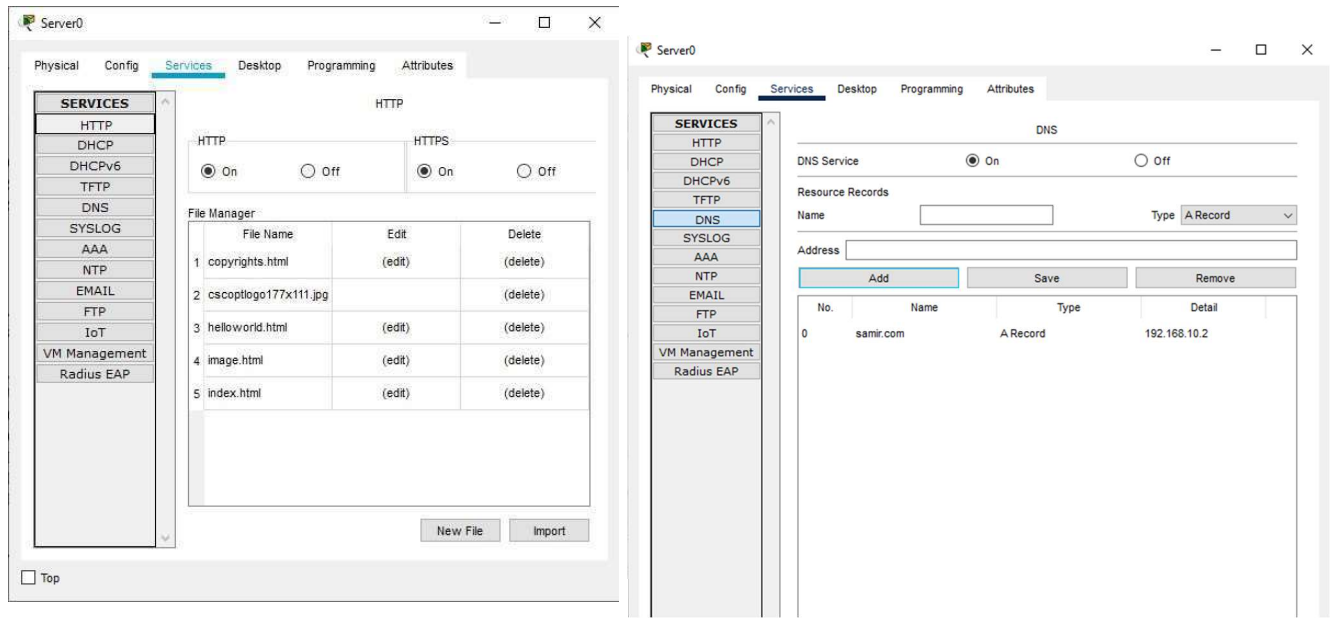
```
Router(config)#access-list [name] [permit/deny] [protocol] [source address]  
[wildcard mask] [destination address] [wildcard mask ] [operator[port]] [log]
```

Application	Port	ACL
FTP	TCP 21	ftp
SSH	TCP 22	ssh
Telnet	TCP 23	telnet
DNS	TCP UDP 53	domain
TFTP	UDP 69	tftp
HTTP	TCP 80	www
NTP	UDP 123	ntp
SNMP	UDP 161	snmp
HTTPS	TCP 443	https

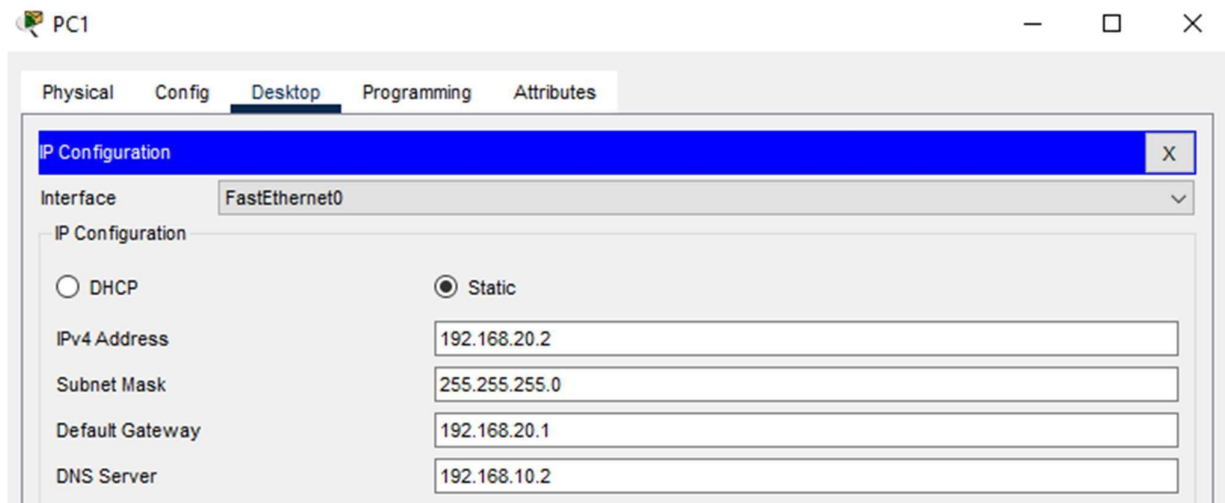
Table: Application Ports Numbers and ACL Keywords

Procedure

- 1.Open Cisco Packet Tracer.
- 2.Set up the network architecture as shown in fig 1.
- 3.Set up the server as:
 - a. Give IP address and gateway to the server.
 - b. Enable the http/https service on the server.



4. Assign IP and Gateway to the computers such that two PCs from 1 switch remains in same network and the other two from next switch remains in another network.

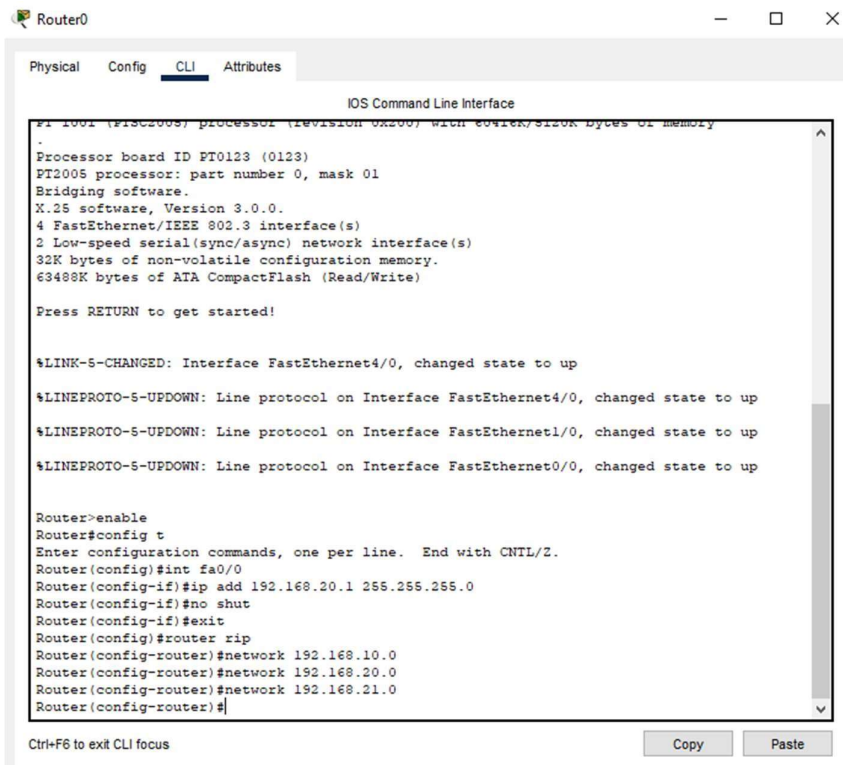


5. Assign the IP address of server in the DNS field of every PCs.
 6. Use CLI of router to assign IP to every interface to which the cable connects in router. And enable the interface.

Command:

Router(config)#int [interface]

Router(config-if)#ip add [ip address] [subnet mask] Router(config-if)#no shut



The screenshot shows a Cisco Router CLI window titled "Router0". The "CLI" tab is selected. The window displays the following text:

```
IOS Command Line Interface
R1 1901 (R13C2005) processor (revision 0x200) with 60736/5120K bytes of memory
.
Processor board ID PT0123 (0123)
PT2005 processor: part number 0, mask 01
Bridging software.
X.25 software, Version 3.0.0.
4 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
63488K bytes of ATA CompactFlash (Read/Write)

Press RETURN to get started!

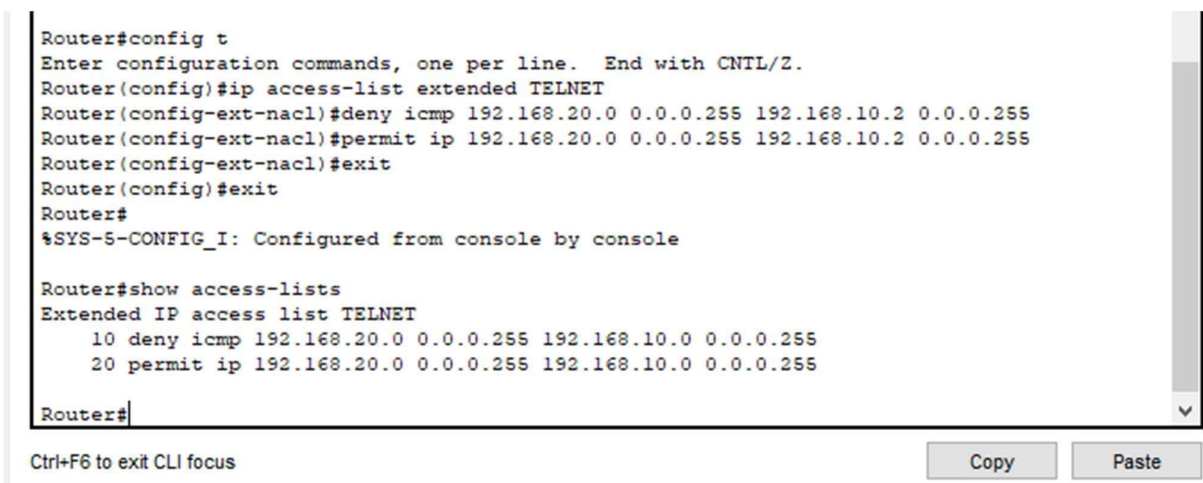
%LINK-5-CHANGED: Interface FastEthernet4/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet4/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa0/0
Router(config-if)#ip add 192.168.20.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 192.168.10.0
Router(config-router)#network 192.168.20.0
Router(config-router)#network 192.168.21.0
Router(config-router)#
```

At the bottom of the window, there is a status bar that says "Ctrl+F6 to exit CLI focus" and two buttons: "Copy" and "Paste".

7. Apply any of the routing protocol i.e., RIP ,OSPF, EIGRP .

8. Now, Create named ACL to deny the ping request but permit the http request in the router for the first network .



The screenshot shows a Cisco Router CLI window with the following text:

```
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip access-list extended TELNET
Router(config-ext-nacl)#deny icmp 192.168.20.0 0.0.0.255 192.168.10.2 0.0.0.255
Router(config-ext-nacl)#permit ip 192.168.20.0 0.0.0.255 192.168.10.2 0.0.0.255
Router(config-ext-nacl)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show access-lists
Extended IP access list TELNET
 10 deny icmp 192.168.20.0 0.0.0.255 192.168.10.2 0.0.0.255
 20 permit ip 192.168.20.0 0.0.0.255 192.168.10.2 0.0.0.255

Router#
```

At the bottom of the window, there is a status bar that says "Ctrl+F6 to exit CLI focus" and two buttons: "Copy" and "Paste".

9. Now, apply the Access-list to the interface on router to which the first network is connected.

```

Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa0/0
Router(config-if)#ip access-group TELNET in
Router(config-if)#exit
Router(config)#

```

Ctrl+F6 to exit CLI focus

Copy

Paste

10. Create another Named ACL for second network to permit ping request and deny http request.

```

Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip access-list extended TELNETT
Router(config-ext-nacl)#deny tcp 192.168.21.0 0.0.0.255 192.168.10.2 0.0.0.255
Router(config-ext-nacl)#permit icmp 192.168.21.0 0.0.0.255 192.168.10.2 0.0.0.255
Router(config-ext-nacl)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show access-lists
Extended IP access list TELNET
 10 deny icmp 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
 20 permit ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
Extended IP access list TELNETT
 10 deny tcp 192.168.21.0 0.0.0.255 192.168.10.0 0.0.0.255
 20 permit icmp 192.168.21.0 0.0.0.255 192.168.10.0 0.0.0.255

Router#

```

Ctrl+F6 to exit CLI focus

Copy

Paste

11. Now, apply this ACL to the interface where second network is connected.

```

Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa1/0
Router(config-if)#ip access-group TELNETT in
Router(config-if)#exit
Router(config)#

```

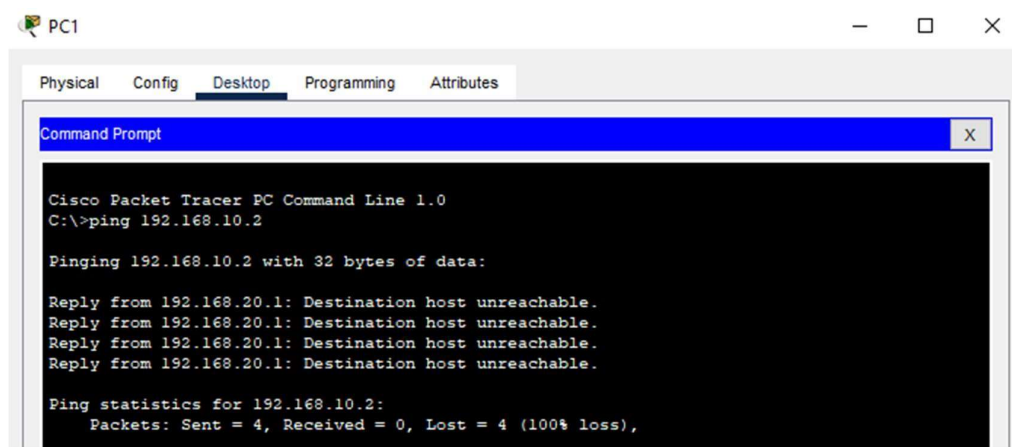
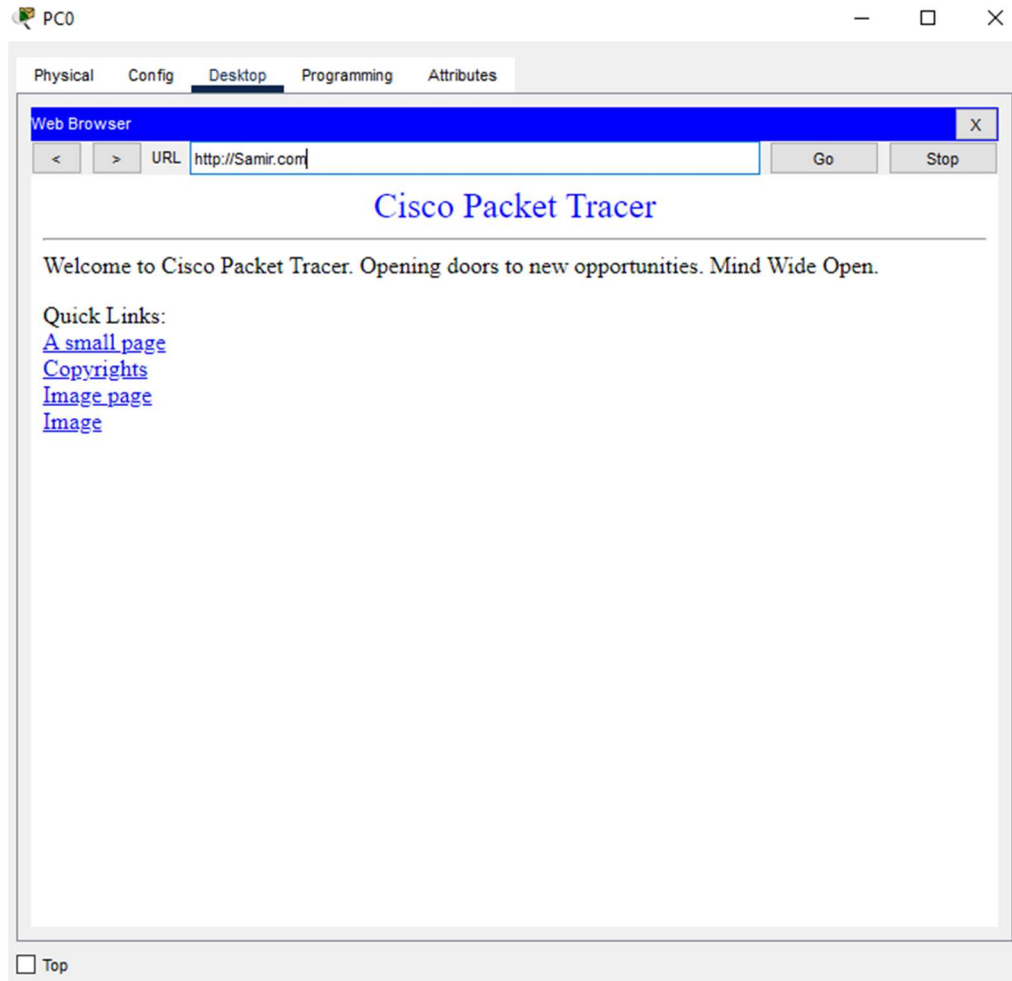
Ctrl+F6 to exit CLI focus

Copy

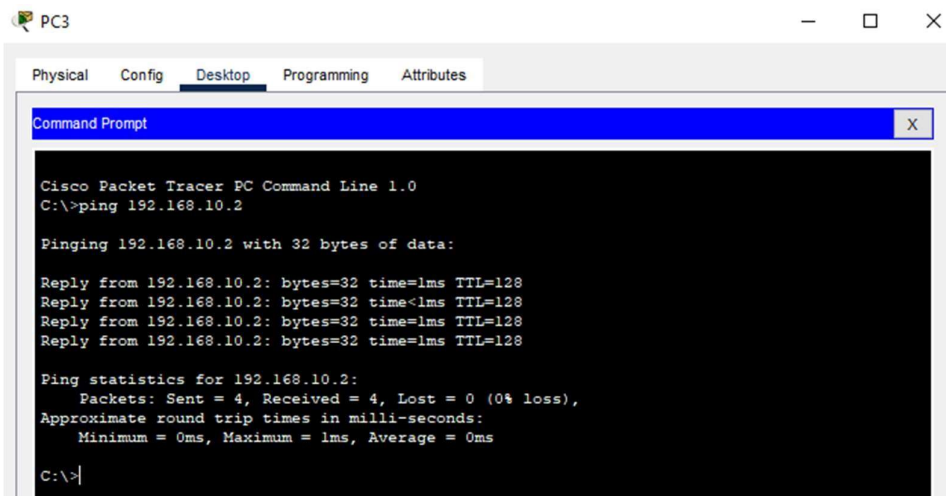
Paste

Examination and Observation

After the successful implementation of ACL NETONE on the router for first network 192.168.10.0, Ping request was denied and http request was permitted.



Similarly, by the implementation of ACL NETTWO on the router for second network 192.168.30.0, Ping request was permitted and http request was denied.



The screenshot shows a Cisco Packet Tracer PC window for PC3. The 'Desktop' tab is active, displaying a 'Command Prompt' window. The command prompt shows the execution of the command 'ping 192.168.10.2'. The output indicates that the ping was successful, with 4 packets sent and 4 received, resulting in 0% loss. The approximate round trip times are shown as Minimum = 0ms, Maximum = 1ms, and Average = 0ms.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Reply from 192.168.10.2: bytes=32 time=1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128
Reply from 192.168.10.2: bytes=32 time=1ms TTL=128
Reply from 192.168.10.2: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>|
```

