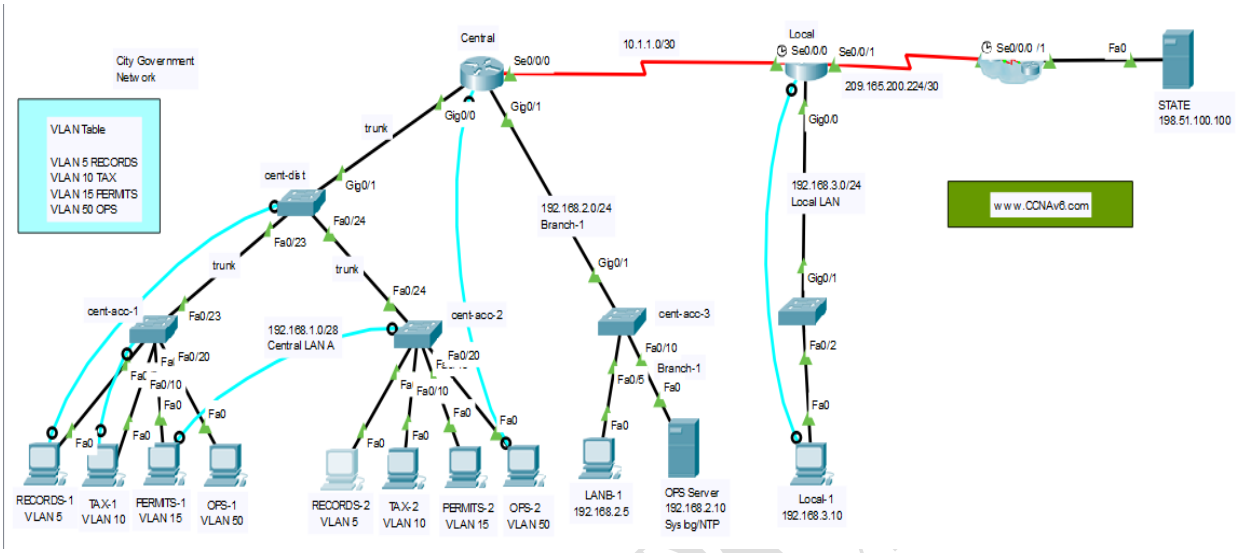
CCNA 2 Practise Skill Assessment Final Happening in Next Day

Required Topology :



How To Solve?

No Matter , We are Here along .

Addressing Table :

Use the following addresses to configure the network. Some addresses are preconfigured on devices

Device	Interface	Network/Address
Central	S0/0/0	10.1.1.1/30
	G0/0.5	192.168.1.0/28 first subnet, first address
	G0/0.10	192.168.1.0/28 second subnet, first address
	G0/0.15	192.168.1.0/28 third subnet, first address
	G0/0.50	192.168.1.0/28 fourth subnet, first address
	G0/1	192.168.2.0/24, first address
cent-dist	SVI	192.168.1.0/28 fourth subnet, any available address
cent-acc-1	SVI	192.168.1.0/28 fourth subnet, any available address
cent-acc-2	SVI	192.168.1.0/28 fourth subnet, any available address
Local	S0/0/0	10.1.1.2/30
	S0/0/1	209.165.200.225/30
	G0/0	192.168.3.1/24
RECORDS-1	NIC	192.168.1.0/28 first subnet, any available address
TAX-1	NIC	192.168.1.0/28 second subnet, any available address
PERMITS-1	NIC	192.168.1.0/28 third subnet, any available address
OPS-1	NIC	192.168.1.0/28 fourth subnet, any available address
RECORDS-2	NIC	192.168.1.0/28 first subnet, any available address
TAX-2	NIC	192.168.1.0/28 second subnet, any available address
PERMITS-2	NIC	192.168.1.0/28 third subnet, any available address
OPS-2	NIC	192.168.1.0/28 fourth subnet, any available address
LANB-1	NIC	192.168.2.5/24
Local-1	NIC	192.168.3.10/24
OPS	NIC	192.168.2.10/24
STATE	NIC	198.51.100.100

VLAN Table

VLAN	Name	Network/Address	Port Assignments
5	RECORDS	192.168.1.0/28 first subnet	cent-acc-1: Fa0/5 cent-acc-2: Fa0/5
10	TAX	192.168.1.0/28 second subnet	cent-acc-1: Fa0/10 cent-acc-2: Fa0/10
15	PERMITS	192.168.1.0/28 third subnet	cent-acc-1: Fa0/15 cent-acc-2: Fa0/15
50	OPS (Management)	192.168.1.0/28 fourth subnet	cent-dist: SVI cent-acc-1: SVI, Fa0/20 cent-acc-2: SVI, Fa0/20

Step1: Basic Device Configuration

Complete a basic device configuration on the **Central** router. Perform the following tasks:

1. Disable DNS lookup.
2. Configure the device with the name shown in the addressing table.
3. Configure password encryption.
4. Assign the encrypted type of privileged EXEC password.
5. Configure a MOTD banner to warn users that unauthorized access is prohibited.
6. Configure the console line so that router status messages will not interrupt command line input.
7. Configure the console to require a password for access.
8. Configure the VTY ports to only accept connections over SSH. Use the following values:

Domain Name: **cisco.com** Local Username: **admin** User Password: **class**Modulus: **1024** Version: **2** The values for your SSH configuration must match these values exactly in order for you to receive credit for your configuration.

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no ip do
Router(config)#no ip domain-lookup
Router(config)#hostname Central
Central(config)#service pass
Central(config)#service password-encryption
Central(config)#enable secret class
Central(config)#banner motd & "Wait Wait !!! Dont't TRy to Access without Passkey " &
Central(config)#line console 0
Central(config-line)#logging synch
Central(config-line)#logging synchronous
Central(config-line)#pass
Central(config-line)#password cisco
Central(config-line)#login
Central(config-line)#exit
Central(config)#ip domain
Central(config)#ip domain-name cisco.com
Central(config)#username admin password class
Central(config)#crypto key gr
Central(config)#crypto key ge
Central(config)#crypto key generate rsa
The name for the keys will be: Central.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 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]

Central(config)#ip ssh version 2
*Mar 1 0:17:58.225: %SSH-5-ENABLED: SSH 1.99 has been enabled
Central(config)#line vty 0 15
Central(config-line)#login local
Central(config-line)#transport inp
Central(config-line)#transport input ssh
Central(config-line)#exit
```

Step 2: Interface Addressing Central

Activate and configure the **G0/1** and **S0/0/0** interfaces of the **Central** router with the IP addresses given in the Addressing Table. The G0/0 interface will be configured later in the assessment.**Configure descriptions for these interfaces**.

```
Central(config)#int g0/1
Central(config-if)#ip add 192.168.2.1 255.255.255.0
Central(config-if)#no shut

Central(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

Central(config-if)#exit
Central(config)#int se0/0/0
Central(config-if)#ip add 10.1.1.1 255.255.255.252
Central(config-if)#no shut

Central(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

Central(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

Central(config-if)#
```

Step 3: VLANs and Trunking

Configure the **cent-dist**, **cent-acc-1**, and **cent-acc-2** switches with VLANs and trunking according to the values in the VLAN table.

1. Add the VLANs to the switches.
2. Name the VLANs exactly as shown in the VLAN table.
3. Configure the links between the cent-dist, cent-acc-1, and cent-acc-2 switches as trunks. Configure the link between cent-dist and Central as a trunk. All trunking interfaces should be statically configured as trunks.
4. Assign the appropriate ports to the VLANs.

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 5
Switch(config-vlan)#name RECORDS
Switch(config-vlan)#vlan 10
Switch(config-vlan)#name TAX
Switch(config-vlan)#vlan PERMITS
                       ^
% Invalid input detected at '^' marker.

Switch(config-vlan)#vlan 15
Switch(config-vlan)#name PERMITS
Switch(config-vlan)#vlan 50
Switch(config-vlan)#name OPS
Switch(config-vlan)#
```

```
cent-acc-1>en
cent-acc-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
cent-acc-1(config)#vlan 5
cent-acc-1(config-vlan)#name RECORDS
cent-acc-1(config-vlan)#vlan 10
cent-acc-1(config-vlan)#name TAX
cent-acc-1(config-vlan)#vlan 15
cent-acc-1(config-vlan)#name PERMITS
cent-acc-1(config-vlan)#vlan 50
cent-acc-1(config-vlan)#name OPS
cent-acc-1(config-vlan)#
```

```
cent-acc-2>en
cent-acc-2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
cent-acc-2(config)#vlan 5
cent-acc-2(config-vlan)#name RECORDS
cent-acc-2(config-vlan)#vlan 10
cent-acc-2(config-vlan)#name TAX
cent-acc-2(config-vlan)#vlan 15
cent-acc-2(config-vlan)#name PERMITS
cent-acc-2(config-vlan)#vlan 50
cent-acc-2(config-vlan)#name OPS
cent-acc-2(config-vlan)#
```

Step 4: Routing Between VLANs

Configure routing between VLANs on the **Central** router. Use the information in the addressing and VLAN tables.

```
Central>en
Password:
Central#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Central(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down

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

Central(config)#int g0/0.5
Central(config-subif)#en
Central(config-subif)#encapsulation dot1q 5
Central(config-subif)#ip add 192.168.1.1 255.255.255.240
Central(config-subif)#int g0/0.10
Central(config-subif)#en
Central(config-subif)#encapsulation dot1q 10
Central(config-subif)#ip add 192.168.1.17 255.255.255.240
Central(config-subif)#int g0/0.15
Central(config-subif)#en
Central(config-subif)#encapsulation dot1q 15
Central(config-subif)#ip add 192.168.1.33 255.255.255.240
Central(config-subif)#int g0/0.50
Central(config-subif)#en
Central(config-subif)#encapsulation dot1q 50
Central(config-subif)#ip add 192.168.1.49 255.255.255.240
Central(config-subif)#int g0/0
Central(config-if)#no shut
Central(config-if)#no shutdown
```

Step 5: Access Control List Configuration

Configure a named standard ACL that meets the following requirements:

15. The list should be named **block15**. The name must match this value exactly in order for you to receive credit for your work.
16. Prevent any host with an address on the **VLAN15**subnetwork from accessing the VTY lines of **Central**.
17. All other hosts should be permitted
18. The list should have two statements. One statement for each requirement in steps 5b and 5c.
19. Place the ACL.

```
Central(config)#ip acc
Central(config)#ip access-list standard block15
Central(config-std-nacl)#deny 192.168.1.32 0.0.0.15
Central(config-std-nacl)#permit any
Central(config-std-nacl)#line vty 0 15
Central(config-line)#acc
Central(config-line)#access-class block15 in
Central(config-line)#exit
Central(config)#
```

Step 6: Switch Virtual Interface (SVI) Configuration

Configure the switch virtual management interfaces on **cent-dist**, **cent-acc-1,**and **cent-acc-2**. Use the information in the addressing and VLAN tables for your configuration. All switches should be reachable from hosts on other networks for the purpose of this assessment.

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int vlan 50
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan50, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan50, changed state to up

Switch(config-if)#ip add 192.168.1.50 255.255.255.240
Switch(config-if)#no shut
Switch(config-if)#exit
Switch(config)#ip de
Switch(config)#ip default-gateway 192.168.1.49
Switch(config)#
```

```
cent-acc-1>en
cent-acc-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
cent-acc-1(config)#int vlan 50
cent-acc-1(config-if)#
%LINK-5-CHANGED: Interface Vlan50, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan50, changed state to up

cent-acc-1(config-if)#ip add 192.168.1.51 255.255.255.240
cent-acc-1(config-if)#no shut
cent-acc-1(config-if)#exit
cent-acc-1(config)#ip de
cent-acc-1(config)#ip default-gateway 192.168.1.49
cent-acc-1(config)#
```

```
cent-acc-2>en
cent-acc-2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
cent-acc-2(config)#int vlan 50
cent-acc-2(config-if)#
%LINK-5-CHANGED: Interface Vlan50, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan50, changed state to up

cent-acc-2(config-if)#ip add 192.168.1.52 255.255.255.2
Bad mask 0xFFFFFF02 for address 192.168.1.52
cent-acc-2(config-if)#ip add 192.168.1.52 255.255.255.240
cent-acc-2(config-if)#no shur
                      ^
% Invalid input detected at '^' marker.

cent-acc-2(config-if)#no shut
cent-acc-2(config-if)#exit
cent-acc-2(config)#ip de
cent-acc-2(config)#ip default-gateway 192.168.1.49
cent-acc-2(config)#
```

Step 7: Switch Port Security Configuration

Improve network security by configuring the **cent-acc-1** switch with the following. You are only required to configure these settings on this one switch for this assessment.

1. Disable ALL unused switch ports.
2. Activate port security on all ports that have hosts connected.
3. Allow only a maximum of two MAC addresses to access the active switch ports.
4. Configure the switch ports to automatically learn the two allowed MAC addresses and record the addresses in the running configuration.
5. Configure the switch ports so that, if the maximum number of addresses for each port is exceeded, packets with unknown source addresses are dropped until a sufficient number of secure MAC addresses are removed. Notification that a violation has occurred is not required.


```
cent-acc-1>en
cent-acc-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
cent-acc-1(config)#int vlan 50
cent-acc-1(config-if)#
%LINK-5-CHANGED: Interface Vlan50, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan50, changed state to up

cent-acc-1(config-if)#ip add 192.168.1.51 255.255.255.240
cent-acc-1(config-if)#no shut
cent-acc-1(config-if)#exit
cent-acc-1(config)#ip de
cent-acc-1(config)#ip default-gateway 192.168.1.49
cent-acc-1(config)#int range fa0/1-4,fa0/6-9,fa0/11-14,fa0/16-19,fa0/24,g0/1-2
cent-acc-1(config-if-range)#shut
cent-acc-1(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down
```

```
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down

%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down
cent-acc-1(config-if-range)#
cent-acc-1(config-if-range)#
cent-acc-1(config-if-range)#exit
cent-acc-1(config)#ip range fa0/5,fa0/10,fa0/15,fa0/20
                   ^
% Invalid input detected at '^' marker.

cent-acc-1(config)#int range fa0/5,fa0/10,fa0/15,fa0/20
cent-acc-1(config-if-range)#switc
cent-acc-1(config-if-range)#switchport por
cent-acc-1(config-if-range)#switchport port-security
cent-acc-1(config-if-range)#swit
cent-acc-1(config-if-range)#switchport port-security maximum 2
cent-acc-1(config-if-range)#switchport port-security mac
cent-acc-1(config-if-range)#switchport port-security mac-address sti
cent-acc-1(config-if-range)#switchport port-security mac-address sticky
cent-acc-1(config-if-range)#switchport port-security vi
cent-acc-1(config-if-range)#switchport port-security violation res
cent-acc-1(config-if-range)#switchport port-security violation restrict
cent-acc-1(config-if-range)#
```

Step 8: Dynamic Routing

Configure RIPv2 routing on **Central** and **Local**.

1. Configure RIPv2 on Central and Local so that all networks are reachable.
2. Configure all LAN physical interfaces so that RIP updates are not sent out to the LANs.
3. Be sure to use the version of RIP that supports classless routing.
4. Prevent RIP from automatically summarizing networks.
5. Configure RIP to automatically send the default route that is already configured on **Local** to **Central.**

```
 "Wait Wait !!! Dont't TRy to Access without Passkey "

User Access Verification

Password:

Central>en
Password:
Central#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Central(config)#router rip
Central(config-router)#version 2
Central(config-router)#no au
Central(config-router)#no auto-summary
Central(config-router)#do 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, 2 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
     192.168.1.0/24 is variably subnetted, 8 subnets, 2 masks
C       192.168.1.0/28 is directly connected, GigabitEthernet0/0.5
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0.5
C       192.168.1.16/28 is directly connected, GigabitEthernet0/0.10
L       192.168.1.17/32 is directly connected, GigabitEthernet0/0.10
C       192.168.1.32/28 is directly connected, GigabitEthernet0/0.15
L       192.168.1.33/32 is directly connected, GigabitEthernet0/0.15
C       192.168.1.48/28 is directly connected, GigabitEthernet0/0.50
L       192.168.1.49/32 is directly connected, GigabitEthernet0/0.50
     192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, GigabitEthernet0/1
L       192.168.2.1/32 is directly connected, GigabitEthernet0/1
```

```
Central(config-router)#
Central(config-router)#do show ip route connected
 C    10.1.1.0/30  is directly connected, Serial0/0/0
 C    192.168.1.0/28  is directly connected, GigabitEthernet0/0.5
 C    192.168.1.16/28  is directly connected, GigabitEthernet0/0.10
 C    192.168.1.32/28  is directly connected, GigabitEthernet0/0.15
 C    192.168.1.48/28  is directly connected, GigabitEthernet0/0.50
 C    192.168.2.0/24  is directly connected, GigabitEthernet0/1

Central(config-router)#network 10.1.1.0
Central(config-router)#network 192.168.1.0
Central(config-router)#network 192.168.1.16
Central(config-router)#network 192.168.1.32
Central(config-router)#network 192.168.1.48
Central(config-router)#network 192.168.2.0
Central(config-router)#pass
Central(config-router)#passive-interface g0/1
Central(config-router)#pass
Central(config-router)#passive-interface g0/0
Central(config-router)#exit
Central(config)#
```

Step 9: Configure Network Monitoring

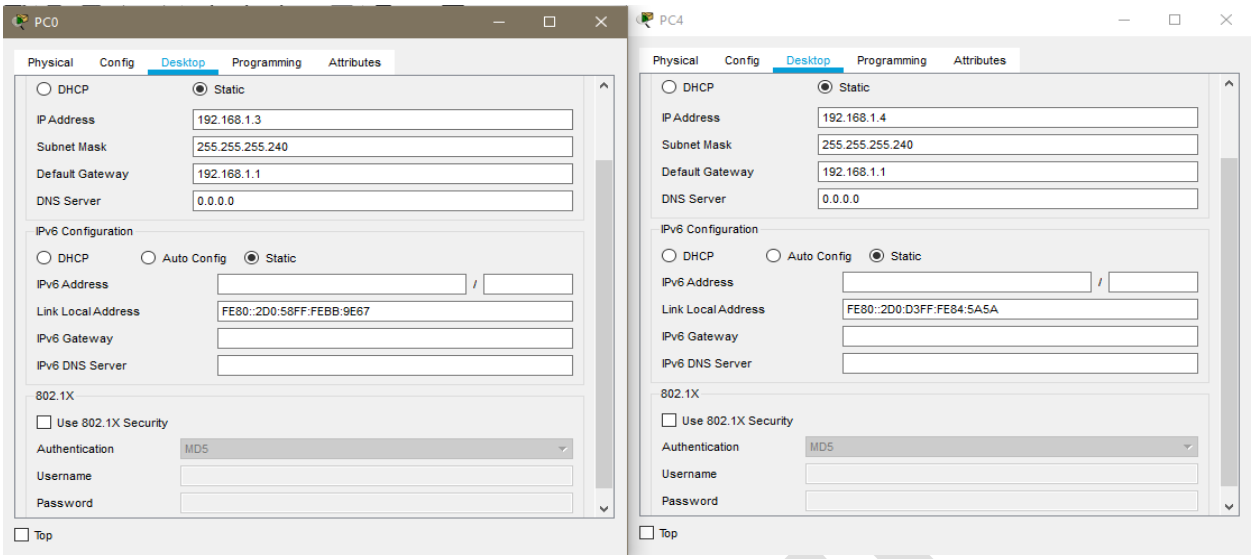
Configure NTP and Syslog server logging on **Central**.

1. Activate the logging and debug timestamp services.
2. Configure **Central**as an NTP client. The NTP server is **OPS** with the address of **192.168.2.10**.
3. Configure Syslog to send **debug level**messages to the **OPS** logging server.

```
Central(config)#
Central(config)#
Central(config)#ser
Central(config)#service ti
Central(config)#service timestamps log
Central(config)#service timestamps log d
Central(config)#service timestamps log datetime m
Central(config)#service timestamps log datetime msec
Central(config)#serv
Central(config)#service t
Central(config)#service timestamps debug
Central(config)#service timestamps debug d
Central(config)#service timestamps debug datetime m
Central(config)#service timestamps debug datetime m
Central(config)#service timestamps debug datetime msec
Central(config)#ntp server
% Incomplete command.
Central(config)#ntp server 192.168.2.0
Central(config)#no ntp server 192.168.2.0
Central(config)#ntp server 192.168.2.10
Central(config)#logging 192.168.2.10
Central(config)#logg
Central(config)#logging trap deb
Central(config)#logging trap debugging
Central(config)#
Central(config)#
```

Step 10: Configure Host Addressing

Address the hosts that are connected to **cent-acc-1** so that they have connectivity to the IP address of the **STATE** server on the Internet. Use the information provided in the Addressing Table.



Repeat the step for three PCs in the same process.

Final Result ;

```
Packet Tracer PC Command Line 1.0
C:\>ping 198.51.100.100

Pinging 198.51.100.100 with 32 bytes of data:

Reply from 198.51.100.100: bytes=32 time=11ms TTL=125
Reply from 198.51.100.100: bytes=32 time=2ms TTL=125
Reply from 198.51.100.100: bytes=32 time=3ms TTL=125
Reply from 198.51.100.100: bytes=32 time=14ms TTL=125

Ping statistics for 198.51.100.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 14ms, Average = 7ms

C:\>
```