Report of Day-11(Security Basics)

What is an access control list (ACL)?

An access control list (ACL) is a list of rules that specifies which users or systems are granted or denied access to a particular object or system resource. Access control lists are also installed in routers or switches, where they act as filters, managing which traffic can access the network.

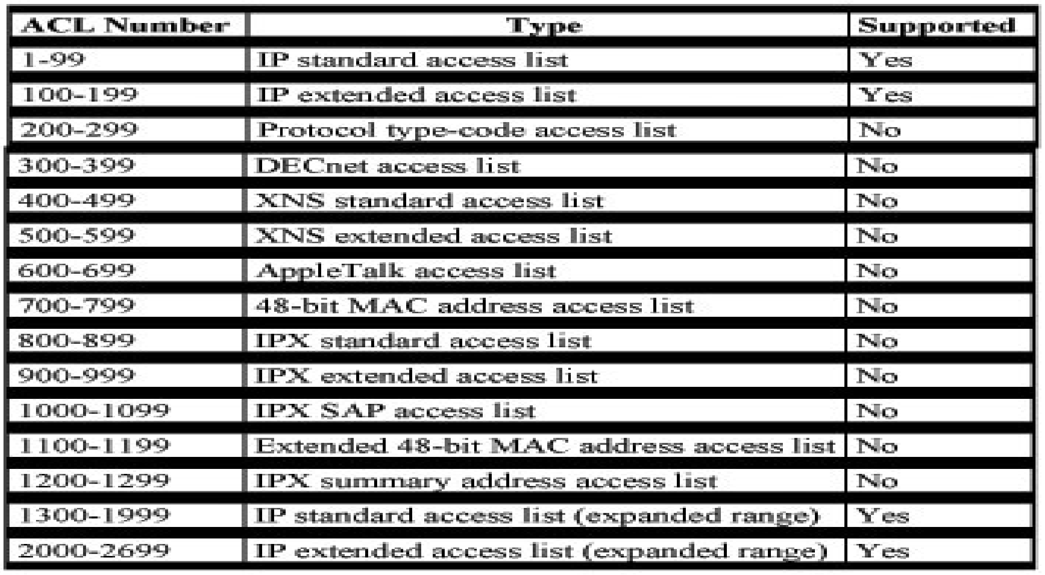
Each system resource has a security attribute that identifies its access control list. The list includes an entry for every user who can access the system. The most common privileges for a file system ACL include the ability to read a file or all the files in a directory, to write to the file or files, and to execute the file if it is an executable file or program. ACLs are also built into network interfaces and operating systems (OSes), including Linux and Windows. On a computer network, access control lists are used to prohibit or allow certain types of traffic to the network. They commonly filter traffic based on its source and destination.

How Do ACLs Work?

Each ACL has one or more access control entries (ACEs) consisting of the name of a user or group of users. The user can also be a role name, such as *programmer* or *tester*. For each of these users, groups or roles, the access privileges are stated in a string of bits called an *access mask*. Generally, the system administrator or the object owner creates the access control list for an object.

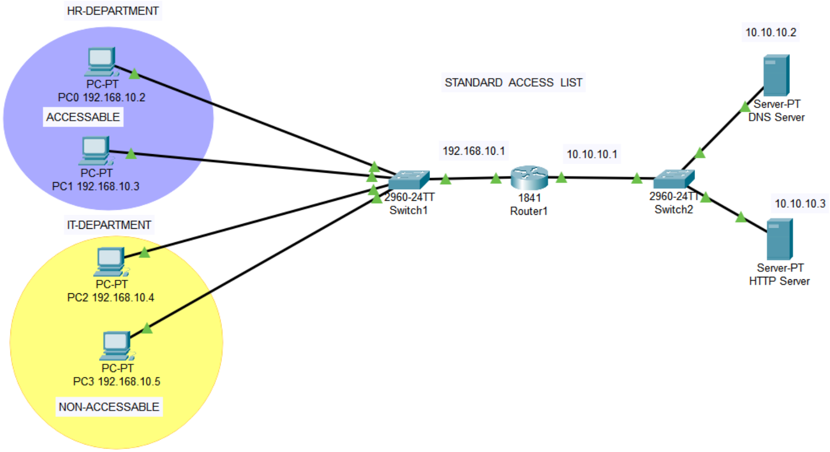
Types Of ACLs:

1) Standard ACL: They block or allow an entire protocol suite using source IP addresses.
2) **Extended ACLs** block or allow network traffic based on a more differentiated set of characteristics that includes source and destination IP addresses and port numbers, as opposed to just source address.

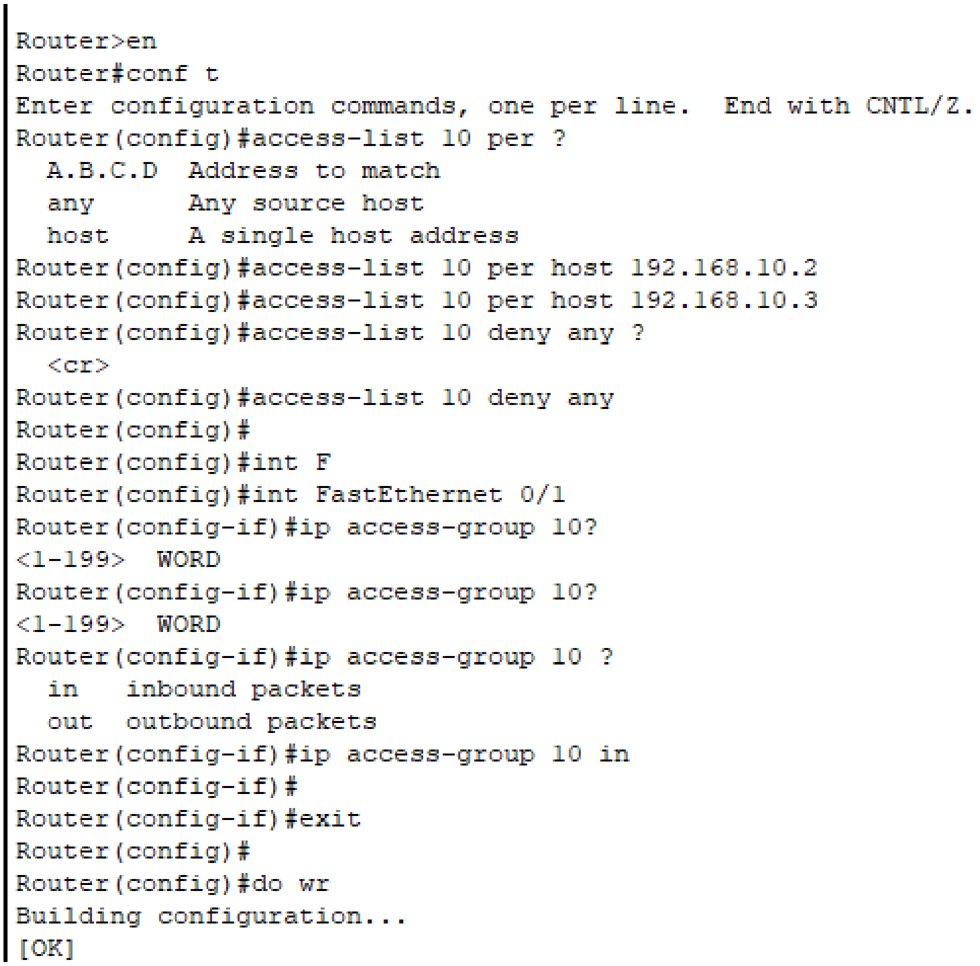


ACL Number	Type	Supported
1-99	IP standard access list	Yes
100-199	IP extended access list	Yes
200-299	Protocol type-code access list	No
300-399	DECnet access list	No
400-499	XNS standard access list	No
500-599	XNS extended access list	No
600-699	AppleTalk access list	No
700-799	48-bit MAC address access list	No
800-899	IPX standard access list	No
900-999	IPX extended access list	No
1000-1099	IPX SAP access list	No
1100-1199	Extended 48-bit MAC address access list	No
1200-1299	IPX summary address access list	No
1300-1999	IP standard access list (expanded range)	Yes
2000-2699	IP extended access list (expanded range)	Yes

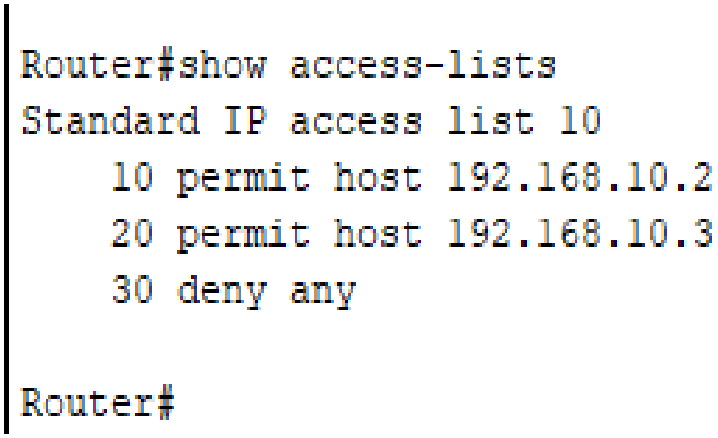
Network Configuration:



Configuring the ACL on the Router:

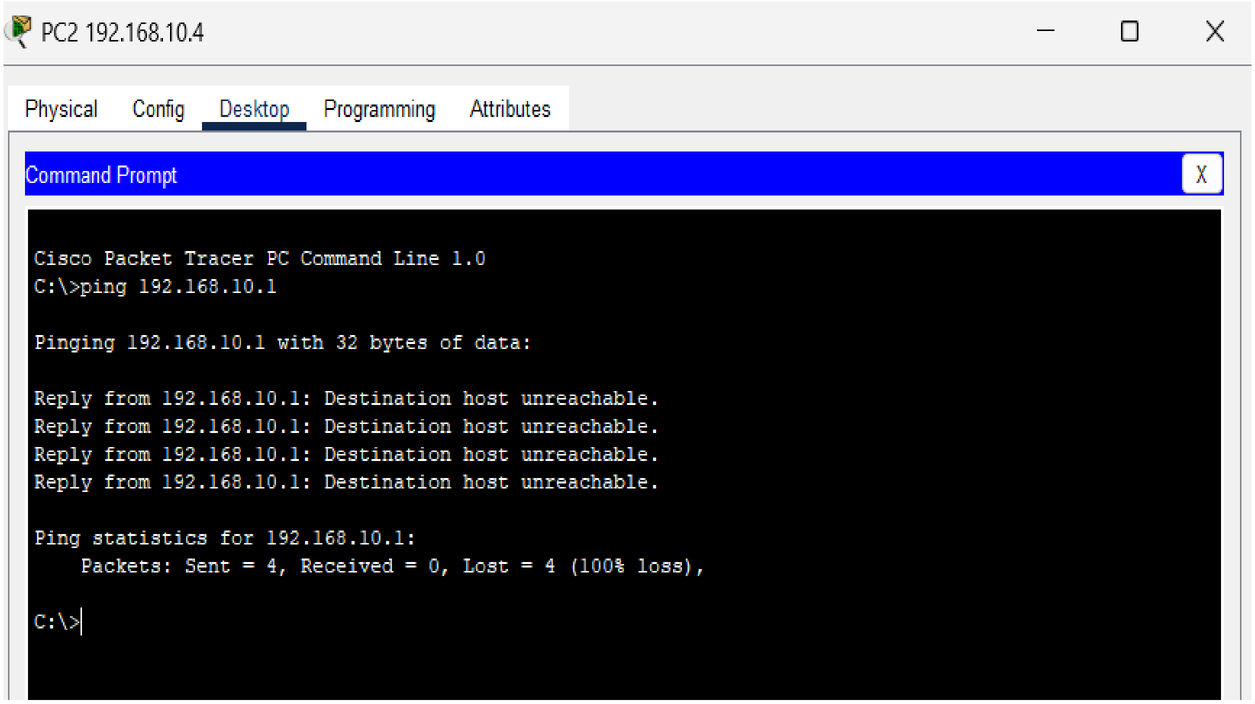


```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 10 per ?
  A.B.C.D  Address to match
  any      Any source host
  host     A single host address
Router(config)#access-list 10 per host 192.168.10.2
Router(config)#access-list 10 per host 192.168.10.3
Router(config)#access-list 10 deny any ?
  <cr>
Router(config)#access-list 10 deny any
Router(config)#
Router(config)#int F
Router(config)#int FastEthernet 0/1
Router(config-if)#ip access-group 10?
<1-199>  WORD
Router(config-if)#ip access-group 10?
<1-199>  WORD
Router(config-if)#ip access-group 10 ?
  in   inbound packets
  out  outbound packets
Router(config-if)#ip access-group 10 in
Router(config-if)#
Router(config-if)#exit
Router(config)#
Router(config)#do wr
Building configuration...
[OK]
```



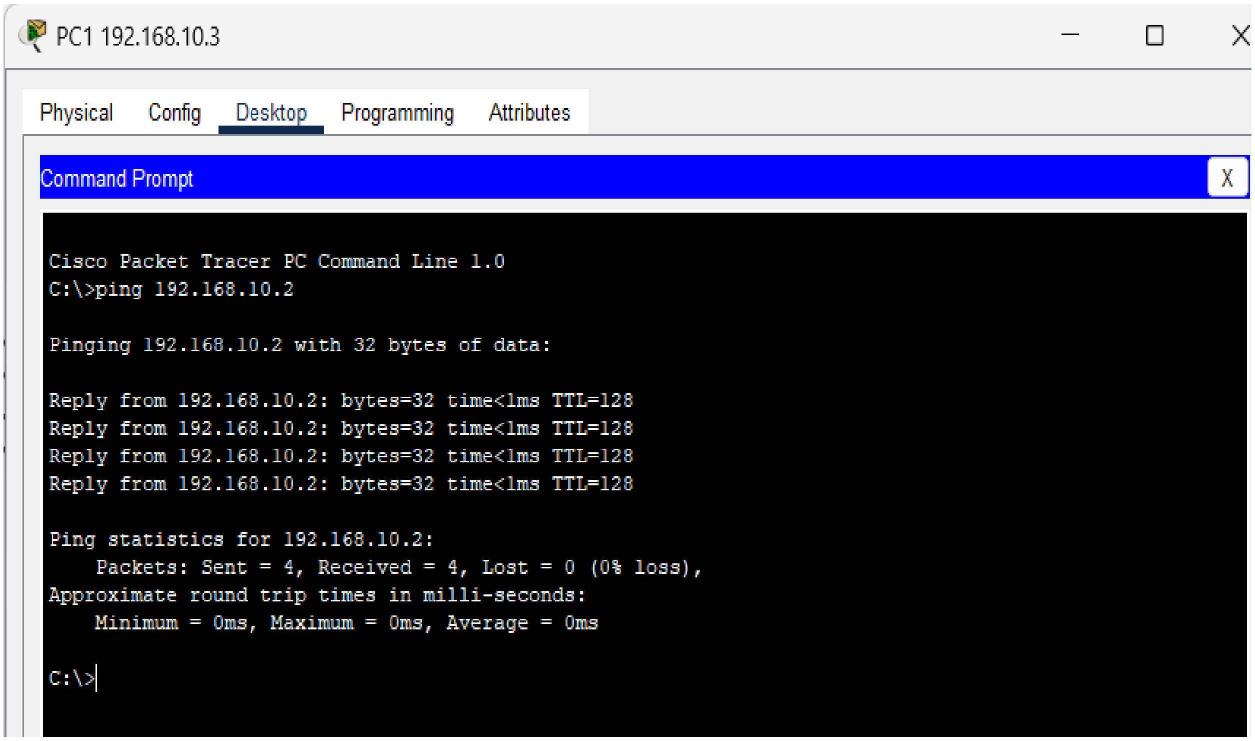
```
Router#show access-lists
Standard IP access list 10
    10 permit host 192.168.10.2
    20 permit host 192.168.10.3
    30 deny any

Router#
```

Pinging from Non-accessible device to Accessible device:



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Pinging from one of the Accessible devices to the Other:

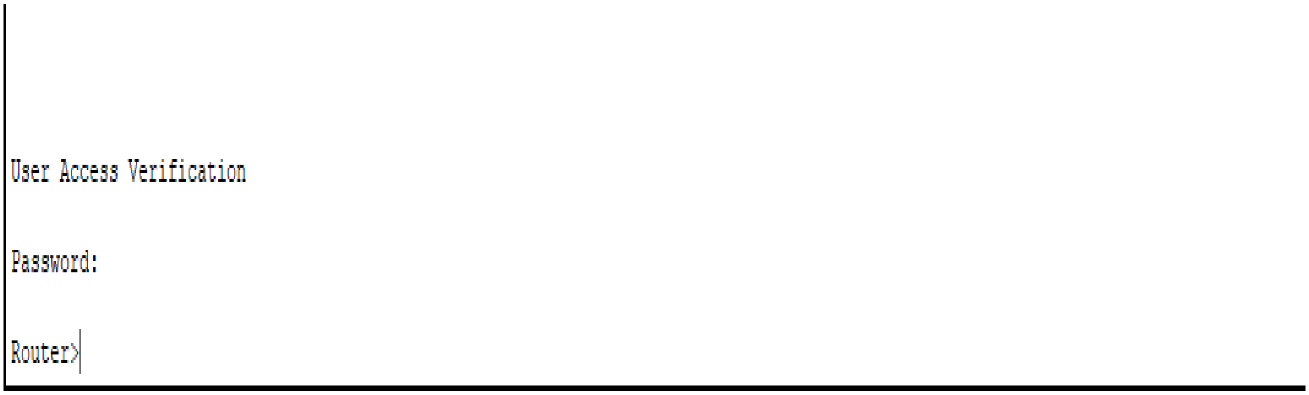


```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.2

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 = 0ms, Average = 0ms

C:\>
```

Setting up the Password for the Console on Router:

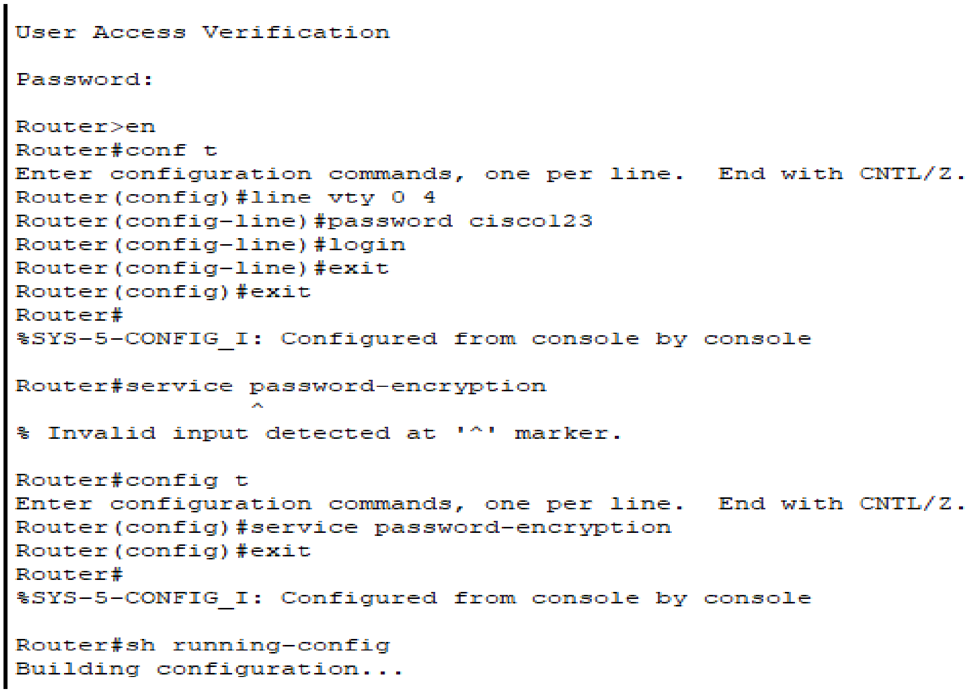
```
Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#line consol 0
Router(config-line)#
Router(config-line)#password 12345
Router(config-line)#login
Router(config-line)#
Router(config-line)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#do write
          ^
% Invalid input detected at '^' marker.

Router#write
Building configuration...
[OK]
Router#
Router#exit
```

Accessing the Console after setting the password on Router:

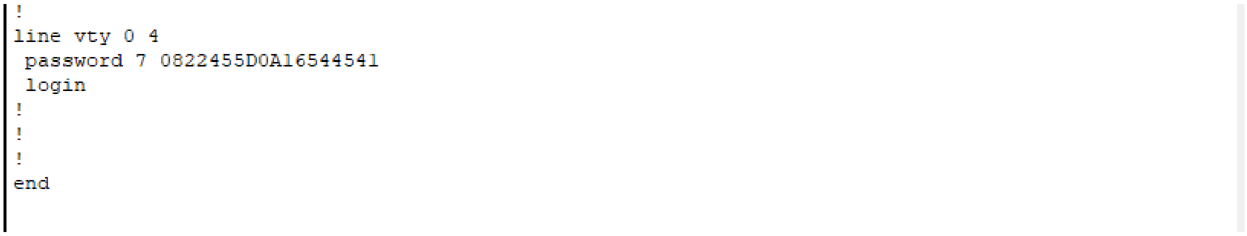


```
User Access Verification

Password:

Router>
```

Configuring the Telnet Password on Router:

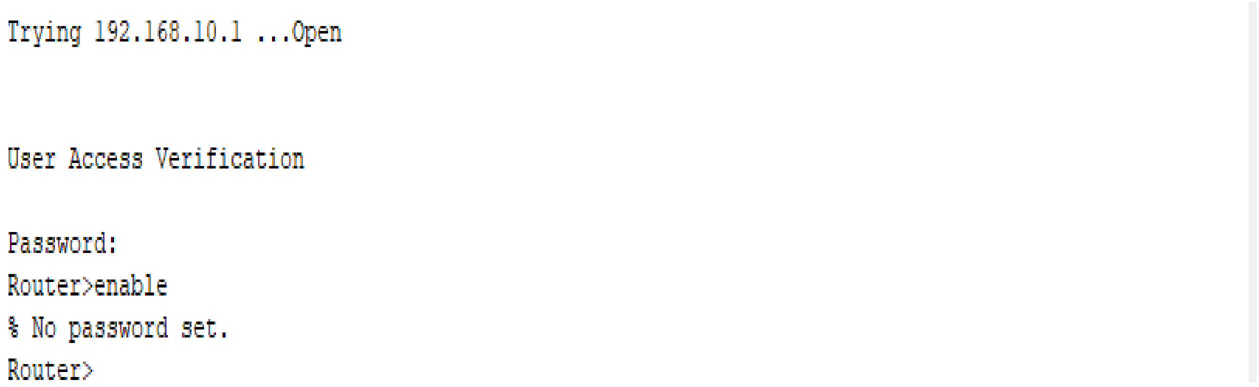


```
User Access Verification

Password:

Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#line vty 0 4
Router(config-line)#password cisco123
Router(config-line)#login
Router(config-line)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#service password-encryption
               ^
% Invalid input detected at '^' marker.

Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#service password-encryption
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#sh running-config
Building configuration...
```



```
!
line vty 0 4
 password 7 0822455D0A16544541
 login
!
!
!
end
```

Accessing the Router After Telnet Configuration:



```
Trying 192.168.10.1 ...Open


User Access Verification

Password:
Router>enable
% No password set.
Router>
```