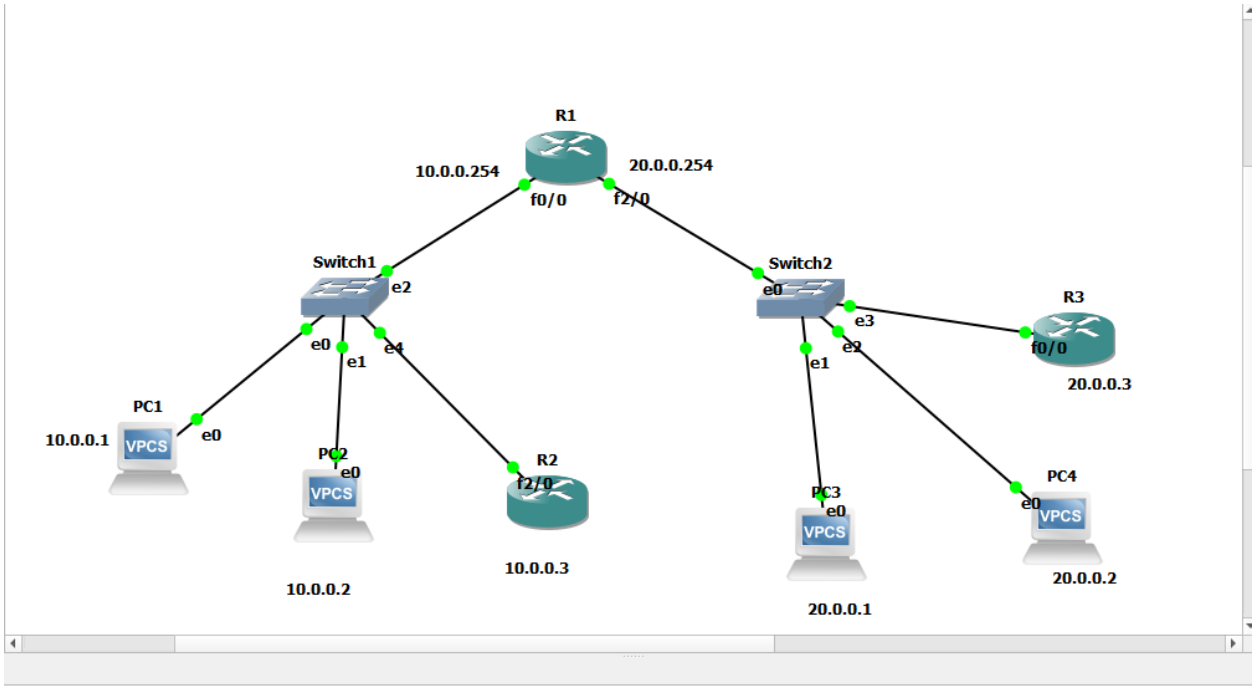
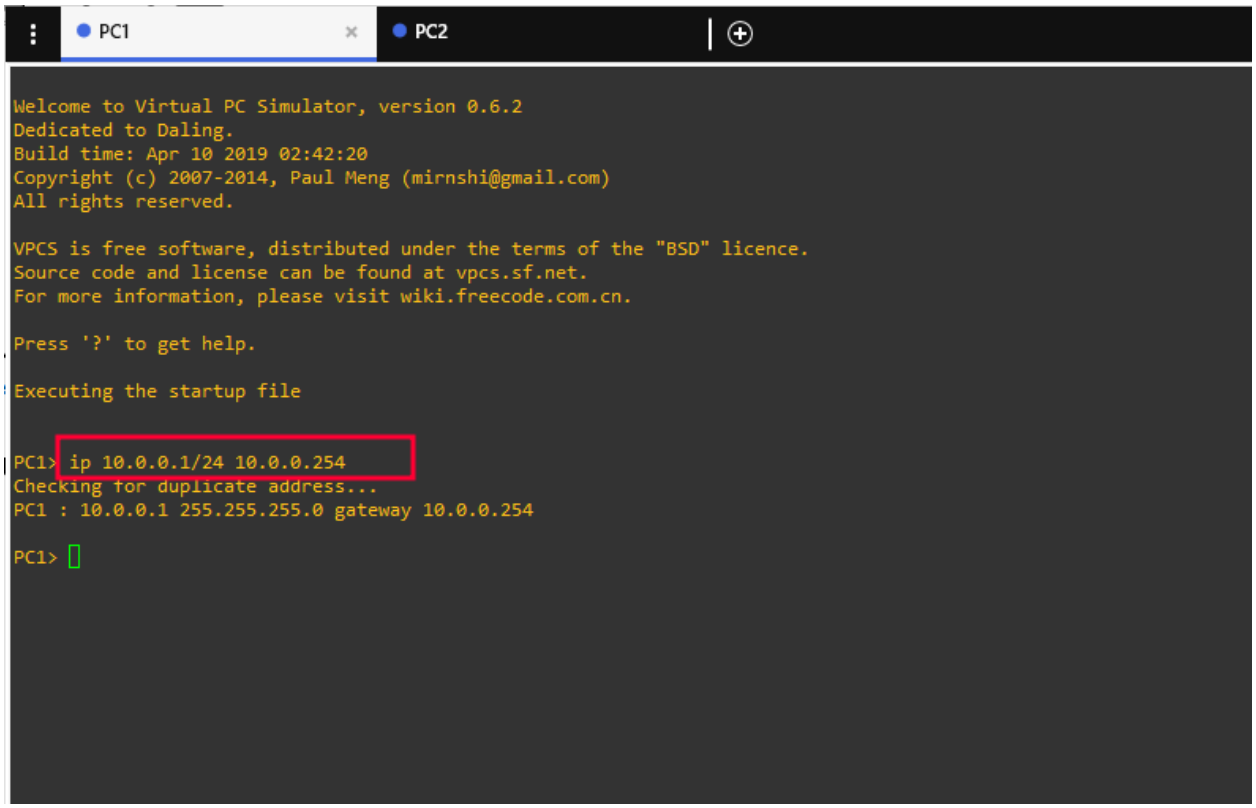
NDC - firefall access list





```
PC2> ip 10.0.0.2/24 10.0.0.254
Checking for duplicate address...
PC1 : 10.0.0.2 255.255.255.0 gateway 10.0.0.254

PC2> show ip

NAME        : PC2[1]
IP/MASK     : 10.0.0.2/24
GATEWAY     : 10.0.0.254
DNS         :
MAC         : 00:50:79:66:68:01
LPORT       : 10024
RHOST:PORT  : 127.0.0.1:10025
MTU:        : 1500

PC2>
```

```
R2#
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface f2/0
R2(config-if)#ip address 10.0.0.3 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#end
R2#
*Jan  6 03:24:15.539: %LINK-3-UPDOWN: Interface FastEthernet2/0, changed state to up
R2#sho
*Jan  6 03:24:16.087: %SYS-5-CONFIG_I: Configured from console by console
*Jan  6 03:24:16.539: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet2/0, changed state to up
R2#show ip int brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            unassigned      YES unset  administratively down down
Serial1/0                  unassigned      YES unset  administratively down down
Serial1/1                  unassigned      YES unset  administratively down down
Serial1/2                  unassigned      YES unset  administratively down down
Serial1/3                  unassigned      YES unset  administratively down down
Serial1/4                  unassigned      YES unset  administratively down down
Serial1/5                  unassigned      YES unset  administratively down down
Serial1/6                  unassigned      YES unset  administratively down down
Serial1/7                  unassigned      YES unset  administratively down down
FastEthernet2/0            10.0.0.3        YES manual up                    up
FastEthernet2/1            unassigned      YES unset  administratively down down
R2#
```

```
to administratively down
R1#
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface f0/0
R1(config-if)#ip address 10.0.0.254 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#end
R1#
*Jan  6 03:25:44.999: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
R1#
*Jan  6 03:25:45.139: %SYS-5-CONFIG_I: Configured from console by console
*Jan  6 03:25:45.999: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R1#
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface f2/0
R1(config-if)#ip address 20.0.0.254 255.255.255.0
R1(config-if)#no shtdown
                ^
% Invalid input detected at '^' marker.

R1(config-if)#no shutdown
R1(config-if)#end
*Jan  6 03:26:51.227: %LINK-3-UPDOWN: Interface FastEthernet2/0, changed state to up
*Jan  6 03:26:52.227: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet2/0, changed state to up
R1(config-if)#end
R1#
*Jan  6 03:26:52.547: %SYS-5-CONFIG_I: Configured from console by console
R1#
```

```
PC3> ip 20.0.0.1/24 20.0.0.254
Checking for duplicate address...
PC1 : 20.0.0.1 255.255.255.0 gateway 20.0.0.254

PC3>
```

```
PC4> ip 20.0.0.2/24 20.0.0.254
Checking for duplicate address...
PC1 : 20.0.0.2 255.255.255.0 gateway 20.0.0.254

PC4>
```

```
R3#
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#interface f0/0
R3(config-if)#ip address 20.0.0.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#end
R3#
*Jan  6 03:30:12.899: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
R3#
*Jan  6 03:30:13.687: %SYS-5-CONFIG_I: Configured from console by console
*Jan  6 03:30:13.899: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R3#
```

```
PC1> ping 10.0.0.3
84 bytes from 10.0.0.3 icmp_seq=1 ttl=255 time=30.165 ms
84 bytes from 10.0.0.3 icmp_seq=2 ttl=255 time=15.287 ms
84 bytes from 10.0.0.3 icmp_seq=3 ttl=255 time=15.177 ms
84 bytes from 10.0.0.3 icmp_seq=4 ttl=255 time=15.283 ms
84 bytes from 10.0.0.3 icmp_seq=5 ttl=255 time=15.242 ms

PC1> ping 10.0.0.254
84 bytes from 10.0.0.254 icmp_seq=1 ttl=255 time=30.068 ms
84 bytes from 10.0.0.254 icmp_seq=2 ttl=255 time=15.381 ms
84 bytes from 10.0.0.254 icmp_seq=3 ttl=255 time=15.205 ms
84 bytes from 10.0.0.254 icmp_seq=4 ttl=255 time=15.212 ms
84 bytes from 10.0.0.254 icmp_seq=5 ttl=255 time=15.214 ms

PC1> ping 20.0.0.1
84 bytes from 20.0.0.1 icmp_seq=1 ttl=63 time=45.081 ms
84 bytes from 20.0.0.1 icmp_seq=2 ttl=63 time=30.304 ms
84 bytes from 20.0.0.1 icmp_seq=3 ttl=63 time=30.165 ms
84 bytes from 20.0.0.1 icmp_seq=4 ttl=63 time=30.150 ms
84 bytes from 20.0.0.1 icmp_seq=5 ttl=63 time=30.256 ms

PC1> ping 20.0.0.3
20.0.0.3 icmp_seq=1 timeout
20.0.0.3 icmp_seq=2 timeout
20.0.0.3 icmp_seq=3 timeout
20.0.0.3 icmp_seq=4 timeout
20.0.0.3 icmp_seq=5 timeout

PC1>
```

```
R2#ping 10.0.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/13/20 ms
R2#ping 20.0.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.0.0.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R2#
```

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ip route 0.0.0.0 0.0.0.0 10.0.0.254
R2(config)#exit
R2#
*Jan  6 03:34:13.835: %SYS-5-CONFIG_I: Configured from console by console
R2#
```

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#ip route 0.0.0.0 0.0.0.0 20.0.0.254
R3(config)#exit
R3#
*Jan  6 03:35:04.111: %SYS-5-CONFIG_I: Configured from console by console
R3#
```

```
R3#ping 10.0.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 32/299/1072 ms
R3#ping 10.0.0.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/56/64 ms
R3#
```

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#access-list 150 deny host 10.0.0.1 20.0.0.0 0.0.0.255
                               ^
% Invalid input detected at '^' marker.

R1(config)#access-list 150 deny icmp host 10.0.0.1 20.0.0.0 0.0.0.255
R1(config)#access-list 150 deny tcp host 10.0.0.3 host 20.0.0.3
R1(config)#access-list 150 permit ip any any
R1(config)#interface f0/0
R1(config-if)#ip access-group 150 in
R1(config-if)#exit
R1(config)#exit
R1#
*Jan  6 04:20:34.475: %SYS-5-CONFIG_I: Configured from console by console
R1#
```

```
PC1> ping 20.0.0.3
*10.0.0.254 icmp_seq=1 ttl=255 time=30.205 ms (ICMP type:3, code:13, Communication administratively prohibited)
*10.0.0.254 icmp_seq=2 ttl=255 time=15.087 ms (ICMP type:3, code:13, Communication administratively prohibited)
*10.0.0.254 icmp_seq=3 ttl=255 time=15.260 ms (ICMP type:3, code:13, Communication administratively prohibited)
*10.0.0.254 icmp_seq=4 ttl=255 time=15.173 ms (ICMP type:3, code:13, Communication administratively prohibited)
*10.0.0.254 icmp_seq=5 ttl=255 time=15.250 ms (ICMP type:3, code:13, Communication administratively prohibited)

PC1>
```

```
R2#
R2#telnet 20.0.0.3
Trying 20.0.0.3 ...
% Destination unreachable; gateway or host down

R2#
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/56/64 ms
R3#
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#line vty 0 4
R3(config-line)#password cdac
R3(config-line)#login
R3(config-line)#
```

```
R1(config)#interface f0/0
R1(config-if)#no ip access-group 150 in
R1(config-if)#exit
R1(config)#
```

Start the capture in wireshark then go to R2

```
% Unknown command or computer name, or unable to fin
R2#telnet 20.0.0.3
Trying 20.0.0.3 ... Open


User Access Verification

Password:
R3>
```