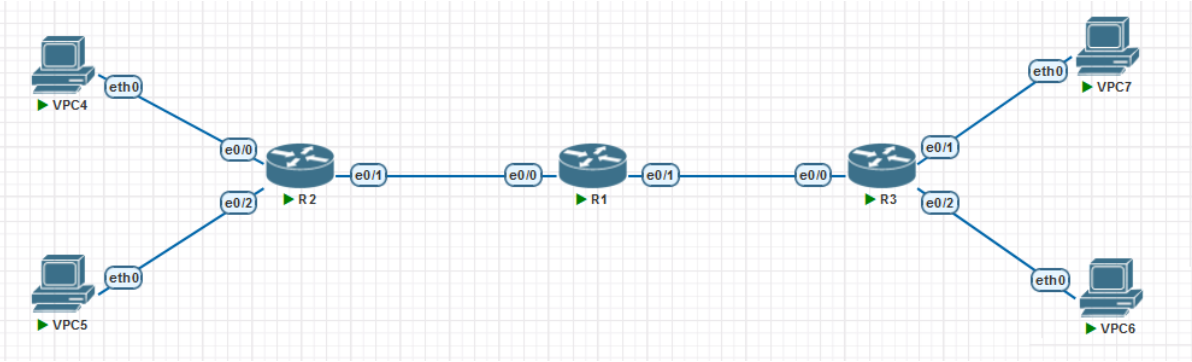
ACL

Use as filter, optionally abandon package from 3rd layer IP addr and 4th layer port number(application). **Basic ACL uses 3rd level IP addr to filter**

Config

Layout and intro



PC4 ---------- PC6 PC4 can connect to PC6

PC4-----|------PC7 PC4 can not connect to PC7

PC5 ---------- PC7 PC5 can connect to PC7

PC5-----|------PC6 PC5 can not connect to PC6

PCs config

VPC4

```
VPCS> ip 4.4.4.4 255.255.255.0 4.4.4.254
Checking for duplicate address...
PC1 : 4.4.4.4 255.255.255.0 gateway 4.4.4.254
```

VPC5

```
VPCS> ip 5.5.5.5 255.255.255.0 5.5.5.254
Checking for duplicate address...
PC1 : 5.5.5.5 255.255.255.0 gateway 5.5.5.254
```

VPC6

```
VPCS> ip 6.6.6.6 255.255.255.0 6.6.6.254
Checking for duplicate address...
PC1 : 6.6.6.6 255.255.255.0 gateway 6.6.6.254
```

VPC7

```
VPCS> ip 7.7.7.7 255.255.255.0 7.7.7.254
Checking for duplicate address...
PC1 : 7.7.7.7 255.255.255.0 gateway 7.7.7.254
```

R1

% Please answer 'yes' or 'no'.

Would you like to enter the initial configuration dialog? [yes/no]: no

Router>en

Router#conf t

Router(config)#hostname R1

R1(config)#interface loopback 0

R1(config-if)#ip address 1.1.1.1 255.255.255.255

R1(config-if)#no shutdown

R1(config)#interface ethernet 0/0

R1(config-if)#no shutdown

R1(config-if)#ip address 12.1.1.1 255.255.255.0

R1(config-if)#exit

R1(config)#interface ethernet 0/1

R1(config-if)#no shutdown

R1(config-if)#ip address 13.1.1.1 255.255.255.0

R1(config-if)#no shutdown

R1(config-if)#exit

R1(config)#end

R1#show ip interface brief

```
R1#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                12.1.1.1        YES manual up                    up
Ethernet0/1                13.1.1.1        YES manual up                    up
Ethernet0/2                unassigned      YES unset  administratively down down
Ethernet0/3                unassigned      YES unset  administratively down down
Loopback0                  1.1.1.1         YES manual up                    up
```

R2

% Please answer 'yes' or 'no'.

Would you like to enter the initial configuration dialog? [yes/no]: no

Router>en

Router#conf t

Router(config)#hostname R2

R2(config)#interface loopback 0

R2(config-if)#no shutdown

R2(config-if)#ip address 2.2.2.2 255.255.255.255

R2(config-if)#exit

R2(config)#interface ethernet 0/1

R2(config-if)#ip address 12.1.1.2 255.255.255.0

R2(config-if)#no shutdown

R2(config-if)#exit

R2(config)#interface ethernet 0/0

R2(config-if)#no shutdown

R2(config-if)#ip address 4.4.4.254 255.255.255.0

R2(config-if)#exit

R2(config)#interface ethernet 0/2

R2(config-if)#ip address 5.5.5.254 255.255.255.0

R2(config-if)#no shutdown

R2(config-if)#end

R2#show ip interface brief

```
R2#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                4.4.4.254       YES manual up                    up
Ethernet0/1                12.1.1.2        YES manual up                    up
Ethernet0/2                5.5.5.254       YES manual up                    up
Ethernet0/3                unassigned      YES unset  administratively down down
Loopback0                  2.2.2.2         YES manual up                    up
```

R3

% Please answer 'yes' or 'no'.

Would you like to enter the initial configuration dialog? [yes/no]: no

Router>en

Router#conf t

Router(config)#hostname R3

R3(config)#interface loopback 0

R3(config-if)#no shutdown

R3(config-if)#ip address 3.3.3.3 255.255.255.255

R3(config-if)#exit

R3(config)#interface ethernet 0/0

R3(config-if)#no shutdown

R3(config-if)#ip address 13.1.1.3 255.255.255.0

R3(config-if)#no shutdown

R3(config-if)#exit

R3(config)#interface ethernet 0/1

R3(config-if)#no shutdown

R3(config-if)#ip address 7.7.7.254 255.255.255.0

R3(config-if)#no shutdown

R3(config-if)#exit

R3(config)#interface ethernet 0/2

R3(config-if)#no shutdown

R3(config-if)#ip address 6.6.6.254 255.255.255.0

R3(config-if)#no shutdown

R3(config-if)#end

R3#show ip interface brief

```
R3#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                13.1.1.3        YES manual up                    up
Ethernet0/1                7.7.7.254       YES manual up                    up
Ethernet0/2                6.6.6.254       YES manual up                    up
Ethernet0/3                unassigned      YES unset  administratively down down
Loopback0                  3.3.3.3         YES manual up                    up
```

OSPF

R1

R1(config)#router ospf 110

R1(config-router)#router-id 1.1.1.1

R1(config-router)#network 1.1.1.1 0.0.0.0 area 0

R1(config-router)#network 12.1.1.1 0.0.0.0 area 0

R1(config-router)#network 13.1.1.1 0.0.0.0 area 0

R1(config-router)#end

R1#show run | section ospf

```
R1#show run | section ospf
router ospf 110
 router-id 1.1.1.1
 network 1.1.1.1 0.0.0.0 area 0
 network 12.1.1.1 0.0.0.0 area 0
 network 13.1.1.1 0.0.0.0 area 0
```

R1#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
       i - IS-IS, su - IS-IS summary, 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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      1.0.0.0/32 is subnetted, 1 subnets
C        1.1.1.1 is directly connected, Loopback0
      2.0.0.0/32 is subnetted, 1 subnets
O        2.2.2.2 [110/11] via 12.1.1.2, 00:04:11, Ethernet0/0
      3.0.0.0/32 is subnetted, 1 subnets
O        3.3.3.3 [110/11] via 13.1.1.3, 00:01:36, Ethernet0/1
      4.0.0.0/24 is subnetted, 1 subnets
O        4.4.4.0 [110/20] via 12.1.1.2, 00:03:31, Ethernet0/0
      5.0.0.0/24 is subnetted, 1 subnets
O        5.5.5.0 [110/20] via 12.1.1.2, 00:03:15, Ethernet0/0
      6.0.0.0/24 is subnetted, 1 subnets
O        6.6.6.0 [110/20] via 13.1.1.3, 00:01:03, Ethernet0/1
      7.0.0.0/24 is subnetted, 1 subnets
O        7.7.7.0 [110/20] via 13.1.1.3, 00:01:20, Ethernet0/1
      12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        12.1.1.0/24 is directly connected, Ethernet0/0
L        12.1.1.1/32 is directly connected, Ethernet0/0
      13.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        13.1.1.0/24 is directly connected, Ethernet0/1
L        13.1.1.1/32 is directly connected, Ethernet0/1
```

R2

R2(config)#router ospf 110

R2(config-router)#router-id 2.2.2.2

R2(config-router)#network 2.2.2.2 0.0.0.0 area 0

R2(config-router)#network 12.1.1.2 0.0.0.0 area 0

R2(config-router)#network 4.4.4.254 0.0.0.0 area 0

R2(config-router)#network 5.5.5.254 0.0.0.0 area 0

R2(config-router)#exit

R2(config)#end

R2#show run | section ospf

```
R2#show run | section ospf
router ospf 110
 router-id 2.2.2.2
 network 2.2.2.2 0.0.0.0 area 0
 network 4.4.4.254 0.0.0.0 area 0
 network 5.5.5.254 0.0.0.0 area 0
 network 12.1.1.2 0.0.0.0 area 0
```

R2#show ip route

```
R1  R2  R3
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
       i - IS-IS, su - IS-IS summary, 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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      1.0.0.0/32 is subnetted, 1 subnets
O        1.1.1.1 [110/11] via 12.1.1.1, 00:04:00, Ethernet0/1
      2.0.0.0/32 is subnetted, 1 subnets
C        2.2.2.2 is directly connected, Loopback0
      3.0.0.0/32 is subnetted, 1 subnets
O        3.3.3.3 [110/21] via 12.1.1.1, 00:01:28, Ethernet0/1
      4.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        4.4.4.0/24 is directly connected, Ethernet0/0
L        4.4.4.254/32 is directly connected, Ethernet0/0
      5.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        5.5.5.0/24 is directly connected, Ethernet0/2
L        5.5.5.254/32 is directly connected, Ethernet0/2
      6.0.0.0/24 is subnetted, 1 subnets
O        6.6.6.0 [110/30] via 12.1.1.1, 00:00:55, Ethernet0/1
      7.0.0.0/24 is subnetted, 1 subnets
O        7.7.7.0 [110/30] via 12.1.1.1, 00:01:11, Ethernet0/1
      12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        12.1.1.0/24 is directly connected, Ethernet0/1
L        12.1.1.2/32 is directly connected, Ethernet0/1
      13.0.0.0/24 is subnetted, 1 subnets
```

R3

R3(config)#router ospf 110

R3(config-router)#router-id 3.3.3.3

R3(config-router)#network 3.3.3.3 0.0.0.0 area 0

R3(config-router)#network 13.1.1.3 0.0.0.0 area 0

R3(config-router)#network 7.7.7.254 0.0.0.0 area 0

R3(config-router)#network 6.6.6.254 0.0.0.0 area 0

R3(config-router)#exit

R3(config)#end

R3#show run | section ospf

```
R3#show run | section ospf
router ospf 110
 router-id 3.3.3.3
 network 3.3.3.3 0.0.0.0 area 0
 network 6.6.6.254 0.0.0.0 area 0
 network 7.7.7.254 0.0.0.0 area 0
 network 13.1.1.3 0.0.0.0 area 0
```

R3#show ip route

```
R1 R2 R3
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
       i - IS-IS, su - IS-IS summary, 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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      1.0.0.0/32 is subnetted, 1 subnets
O        1.1.1.1 [110/11] via 13.1.1.1, 00:00:58, Ethernet0/0
      2.0.0.0/32 is subnetted, 1 subnets
O        2.2.2.2 [110/21] via 13.1.1.1, 00:00:58, Ethernet0/0
      3.0.0.0/32 is subnetted, 1 subnets
C        3.3.3.3 is directly connected, Loopback0
      4.0.0.0/24 is subnetted, 1 subnets
O        4.4.4.0 [110/30] via 13.1.1.1, 00:00:58, Ethernet0/0
      5.0.0.0/24 is subnetted, 1 subnets
O        5.5.5.0 [110/30] via 13.1.1.1, 00:00:58, Ethernet0/0
      6.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        6.6.6.0/24 is directly connected, Ethernet0/2
L        6.6.6.254/32 is directly connected, Ethernet0/2
      7.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        7.7.7.0/24 is directly connected, Ethernet0/1
L        7.7.7.254/32 is directly connected, Ethernet0/1
      12.0.0.0/24 is subnetted, 1 subnets
O        12.1.1.0 [110/20] via 13.1.1.1, 00:00:58, Ethernet0/0
      13.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        13.1.1.0/24 is directly connected, Ethernet0/0
```

ACL

R2#conf t

R2(config)#access-list 100 deny ip 4.4.4.4 0.0.0.0 7.7.7.7 0.0.0.0

R2(config)#access-list 100 deny ip host 5.5.5.5 host 6.6.6.6

R2(config)#access-list 100 permit ip any any

R2(config)#end

Extended IP access list 100

```
R2#show ip access-lists
Extended IP access list 100
    10 deny ip host 4.4.4.4 host 7.7.7.7
    20 deny ip host 5.5.5.5 host 6.6.6.6
    30 permit ip any any
```

R2#conf t

R2(config)#interface ethernet 0/1

R2(config-if)#ip access-group 100 out

R2(config-if)#no shutdown

R2(config-if)#end

R2#show ip interface ethernet 0/1

```
R2#show ip interface ethernet 0/1
Ethernet0/1 is up, line protocol is up
  Internet address is 12.1.1.2/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.5 224.0.0.6
  Outgoing access list is 100
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP CEF switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
```

Result

VPC4

```
VPCS> ping 6.6.6.6

84 bytes from 6.6.6.6 icmp_seq=1 ttl=61 time=3.413 ms
84 bytes from 6.6.6.6 icmp_seq=2 ttl=61 time=1.721 ms
ping 84 bytes from 6.6.6.6 icmp_seq=3 ttl=61 time=0.889 ms
7.7.84 bytes from 6.6.6.6 icmp_seq=4 ttl=61 time=1.001 ms
7.784 bytes from 6.6.6.6 icmp_seq=5 ttl=61 time=0.875 ms

VPCS> ping 7.7.7.7

*4.4.4.254 icmp_seq=1 ttl=255 time=0.278 ms (ICMP type:3, code:13, Communication administrativel
y prohibited)
*4.4.4.254 icmp_seq=2 ttl=255 time=0.697 ms (ICMP type:3, code:13, Communication administrativel
y prohibited)
*4.4.4.254 icmp_seq=3 ttl=255 time=0.469 ms (ICMP type:3, code:13, Communication administrativel
y prohibited)
*4.4.4.254 icmp_seq=4 ttl=255 time=0.331 ms (ICMP type:3, code:13, Communication administrativel
y prohibited)
*4.4.4.254 icmp_seq=5 ttl=255 time=0.426 ms (ICMP type:3, code:13, Communication administrativel
y prohibited)
```

VPC5

```
VPCS> ping 7.7.7.7

84 bytes from 7.7.7.7 icmp_seq=1 ttl=61 time=2.256 ms
84 bytes from 7.7.7.7 icmp_seq=2 ttl=61 time=2.083 ms
84 bytes from 7.7.7.7 icmp_seq=3 ttl=61 time=1.552 ms
84 bytes from 7.7.7.7 icmp_seq=4 ttl=61 time=1.705 ms
84 bytes from 7.7.7.7 icmp_seq=5 ttl=61 time=1.143 ms

VPCS> ping 6.6.6.6

*5.5.5.254 icmp_seq=1 ttl=255 time=0.520 ms (ICMP type:3, code:13, Communication administrativel
y prohibited)
*5.5.5.254 icmp_seq=2 ttl=255 time=0.474 ms (ICMP type:3, code:13, Communication administrativel
y prohibited)
*5.5.5.254 icmp_seq=3 ttl=255 time=1.424 ms (ICMP type:3, code:13, Communication administrativel
y prohibited)
*5.5.5.254 icmp_seq=4 ttl=255 time=0.828 ms (ICMP type:3, code:13, Communication administrativel
y prohibited)
*5.5.5.254 icmp_seq=5 ttl=255 time=0.502 ms (ICMP type:3, code:13, Communication administrativel
y prohibited)
```