LAN-1
192.168.20.0/24

PC-PT
PC-B
Fa0

PC-PT
PC-A
Fa0

Fa0/2

Fa0/1

2960...

Gig0/1

Gig0/0

1941
R2

Se0/1/0

Gig0/1

PC-PT
PC-C (MGMT)
Fa0

Fa0/1

Gig0/1

2960-24TT
S2

LAN-2
192.168.24.0/24

10.10.10.0/30

Server-PT
HTTP/DNS Server 192.168.10.10/32

Fa0

LAN-Server
192.168.10.0/24

Gig0/0

fa0/1

Se0/1/0

Se0/0/0

209.86.120.84/30

10.10.11.0/30

Se0/1/1

1 Gig0/0
R3

Gig0/1

2960...
S1

Fa0/3

Fa0/1

Fa0/2

PC-PT
PC-F
Fa0

PC-PT
Fa0

PC-PT
PC-E
Fa0

LAN-3
192.168.30.0/24

Se0/0/0
ISP

LAN-1
VLAN 20 = UFFICIO 192.168.20.0/24

LAN-2
VLAN 24 = GARAGE 192.168.24.0/24
VLAN 88 = NATIVA
VLAN 91 = MGMT
192.168.91.0/24
VLAN 88 = NATIVA

LAN-3
VLAN 92 = MGMT
192.168.92.0/24
VLAN30 = HR 192.168.30.0/24
VLAN 88
VLAN 93 = MGMT 192.168.93.0/24

Configurare OSPF per la condivisione delle rotte e le seguenti ACL:
- ACL standard che impedisca l'accesso degli host della LAN 3 al Router ISP;
-ACL extended che permette solo ai dispositivi della LAN-3 di usare il servizio DNS del Server.
- ACL extended che nega il servizio HTTP del server a PC-E ma non agli altri PC della LAN-3.
- ACL extended che impedisce il ping dalle LAN-1 e LAN-2 verso la LAN-3, ma sia la LAN-1 e LAN-2 possono pingare tutto il resto(che possono quindi pingare liberamente);
-ACL per consentire solo alle LAN-1 e LAN-2 di comunicare con LAN-3 usando SSH (no telnet).

ROUTER 1

PC-PT
PC-A

Fa0

Fa0/1

Fa0/2

Server-PT
HTTP/DNS Server 192.168.10.10/32

Fa0

LAN-Server
192.168.10.0/24

10.10.10.0/30

Gig0/0

Fa0/1

Se0/1/0

Se0/0/0

10.10.11.0/30

Se0/1/1
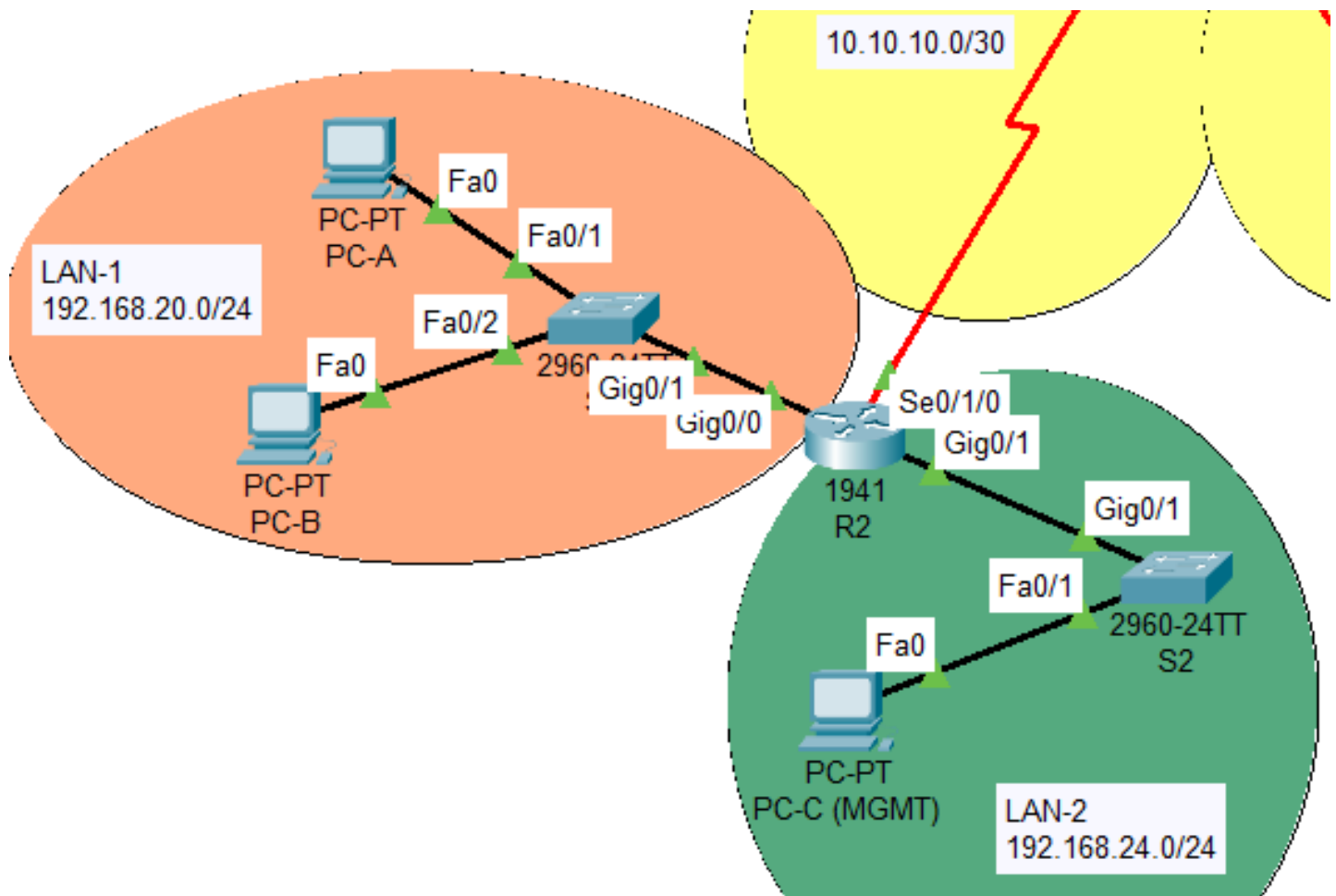
209.86.120.84/30

Fa0/1

Fa0

PC-PT

Se0/0/0

ISP
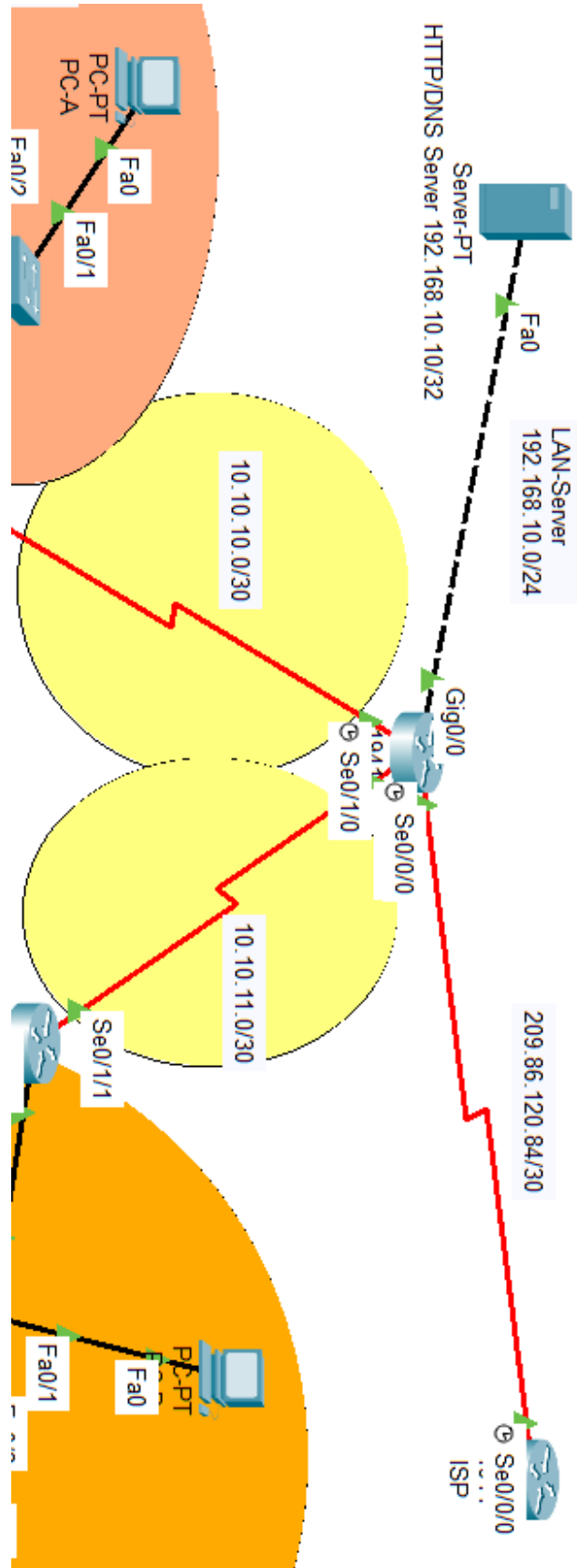
ROUTER 1

```
R1(config)# interface g0/0
R1(config-if)# description "LINK TO SERVER"
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface s0/0/0
R1(config-if)# description "LINK TO INTERNET"
R1(config-if)# ip address 209.86.120.85 255.255.255.252
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface s0/1/0
R1(config-if)# description "LINK TO R2"
R1(config-if)# ip address 10.10.10.1 255.255.255.252
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface s0/1/1
R1(config-if)# description "LINK TO R3"
R1(config-if)# ip address 10.10.11.1 255.255.255.252
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# ip route 0.0.0.0 0.0.0.0 209.86.120.86
// DHCP
R1(config)# ip dhcp excluded-address 192.168.20.1 192.168.20.9
R1(config)# ip dhcp excluded-address 192.168.24.1 192.168.24.9
R1(config)# ip dhcp excluded-address 192.168.30.1 192.168.30.9
R1(config)# ip dhcp pool "VLAN-1_Pool"
R1(dhcp-config)# network 192.168.20.0 255.255.255.0
R1(dhcp-config)# default-router 192.168.20.1
R1(dhcp-config)# dns-server 192.168.10.10
R1(dhcp-config)# domain-name "cisco.com"
R1(dhcp-config)# exit
R1(config)# ip dhcp pool "VLAN-2_Pool"
R1(dhcp-config)# network 192.168.24.0 255.255.255.0
R1(dhcp-config)# default-router 192.168.24.1
R1(dhcp-config)# dns-server 192.168.10.10
R1(dhcp-config)# domain-name "cisco.com"
R1(dhcp-config)# exit
R1(config)# ip dhcp pool VLAN-3_Pool
R1(dhcp-config)# network 192.168.30.0 255.255.255.0
R1(dhcp-config)# default-router 192.168.30.1
R1(dhcp-config)# dns-server 192.168.10.10
R1(dhcp-config)# domain-name "cisco.com"
R1(dhcp-config)# exit
```

```
// OSPF
R1(config)# router ospf 10
R1(config-router)# router-id 1.1.1.1
R1(config-router)# network 192.168.10.0 0.0.0.255 area 0
R1(config-router)# network 10.10.10.0 0.0.0.3 area 0
R1(config-router)# network 10.10.11.0 0.0.0.3 area 0
R1(config-router)# passive-interface g0/0
R1(config-router)# passive-interface s0/0/0
R1(config-router)# exit
R1(config)# interface s0/1/0
R1(config-if)# ip ospf network point-to-point
R1(config-if)# exit
R1(config)# interface s0/1/1
R1(config-if)# ip ospf network point-to-point
R1(config-if)# exit
// ACL
R1(config)# access-list 10 deny 192.168.30.0 0.0.0.255
R1(config)# access-list 10 permit any
R1(config)# interface s0/0/0
R1(config-if)# ip access-group 10 out
R1(config-if)# exit
R1(config)# router ospf 10
R1(config-router)# default-information originate
R1(config-router)# exit
R1(config)# ip access-list extended SSH_ONLY
R1(config-ext-nacl)# remark "PERMETTO LAN-1 e LAN-2 di COLLEGARSI in SSH a LAN-3"
R1(config-ext-nacl)# permit tcp 192.168.20.0 0.0.0.255 192.168.93.0 0.0.0.255 eq 22
R1(config-ext-nacl)# permit tcp 192.168.24.0 0.0.0.255 192.168.93.0 0.0.0.255 eq 22
R1(config-ext-nacl)# deny tcp any 192.168.93.0 0.0.0.255 eq 22
R1(config-ext-nacl)# deny tcp any 192.168.93.0 0.0.0.255 eq 23 (telnet)
R1(config-ext-nacl)# permit ip any any
R1(config-ext-nacl)# exit
R1(config)# interface s0/1/1
R1(config-if)# ip access-group SSH_ONLY out
R1(config-if)# exit
R1(config)#
```

ROUTER 2

10.10.10.0/30

LAN-1
192.168.20.0/24

Fa0
PC-PT
PC-A

Fa0/1

Fa0/2

Fa0
PC-PT
PC-B

2960

Gig0/1
Gig0/0

Se0/1/0
Gig0/1

1941
R2

Gig0/1

Fa0/1

2960-24TT
S2

Fa0
PC-PT
PC-C (MGMT)

LAN-2
192.168.24.0/24

```
R2(config)# interface g0/0
R2(config-if)# description "DEFAULT-GATEWAY OF LAN-1"
R2(config-if)# ip address 192.168.20.1 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)# exit
R2(config)# interface g0/1
R2(config-if)# description "DEFAULT-GATEWAY OF LAN-2"
R2(config-if)# ip address 192.168.24.1 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)# exit
R2(config)# interface s0/1/0
R2(config-if)# description "LINK TO R1"
R2(config-if)# ip address 10.10.10.2 255.255.255.252
R2(config-if)# no shutdown
R2(config-if)# exit
// DHCP
R2(config)# interface g0/0
R2(config-if)# ip helper-address 10.10.10.1
R2(config-if)# exit
R2(config)# interface g0/1
R2(config-if)# ip helper-address 10.10.10.1
R2(config-if)# exit
// OSPF
R2(config)# router ospf 10
R2(config-router)# router-id 2.2.2.2
R2(config-router)# network 10.10.10.0 0.0.0.3 area 0
R2(config-router)# network 192.168.20.0 0.0.0.255 area 0
R2(config-router)# network 192.168.24.0 0.0.0.255 area 0
R2(config-router)# passive-interface g0/0
R2(config-router)# passive-interface g0/1
R2(config-router)# exit
R2(config)# interface s0/1/0
R2(config-if)# ip ospf network point-to-point
R2(config-if)# exit
R2(config)# router ospf 10
R2(config-router)# default-information originate
R2(config-router)# exit
// ACL
R2(config)# ip access-list extended "BLOCK-LAN1"
R2(config-ext-nacl)# remark "BLOCCO DNS a LAN-3"
R2(config-ext-nacl)# deny udp 192.168.20.0 0.0.0.255 host 198.160.10.10 eq 53 (domain)
R2(config-ext-nacl)# deny icmp 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255 echo
R2(config-ext-nacl)# permit ip any any
```
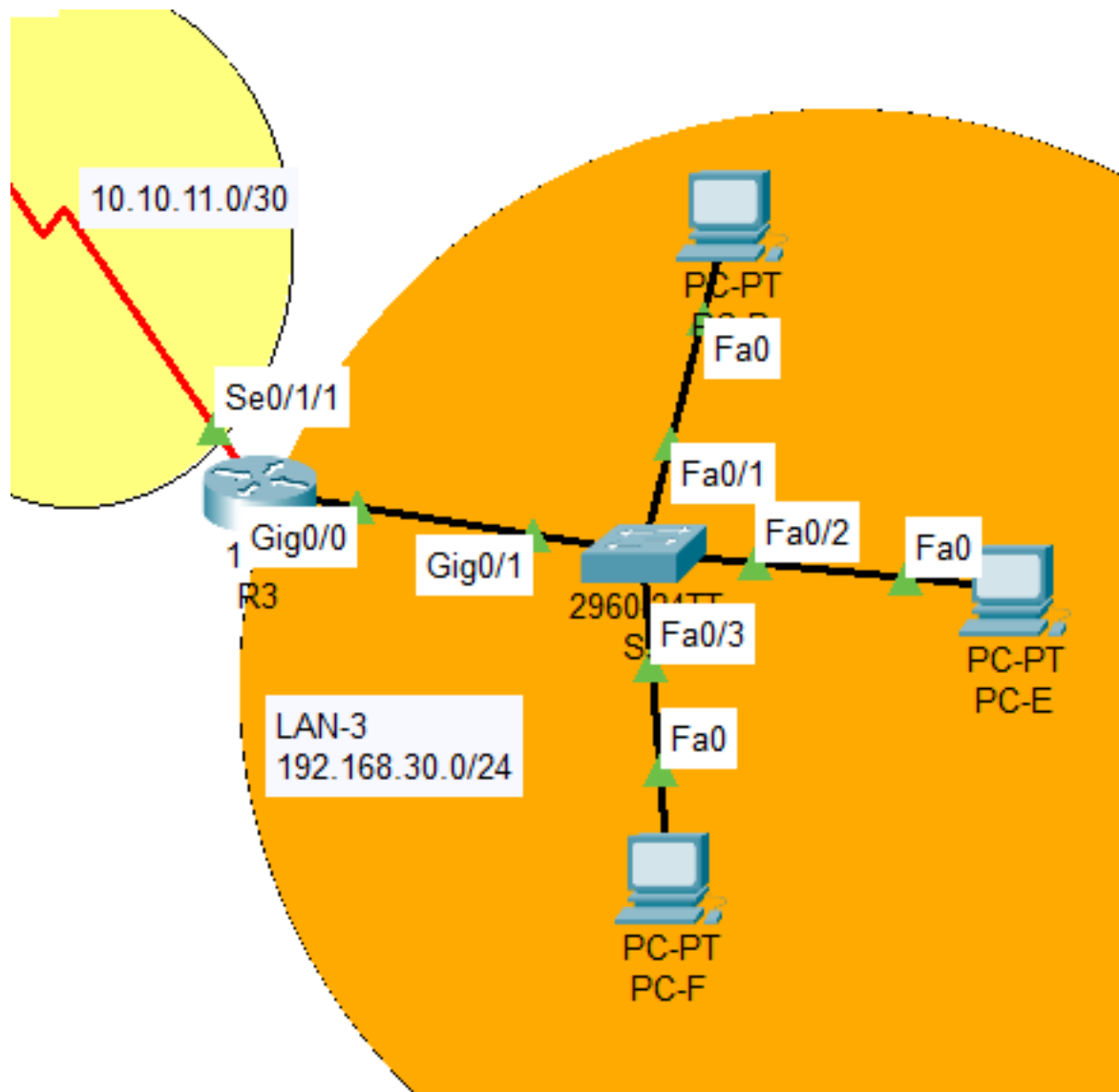
```
R2(config-ext-nacl)# exit
R2(config)# ip access-list extended "BLOCK-LAN2"
R2(config-ext-nacl)# remark "BLOCCO DNS a LAN-2"
R2(config-ext-nacl)# deny udp 192.168.24.0 0.0.0.255 host 198.160.10.10 eq 53 (domain)
R2(config-ext-nacl)# deny icmp 192.168.24.0 0.0.0.255 192.168.30.0 0.0.0.255 echo
R2(config-ext-nacl)# permit ip any any
R2(config-ext-nacl)# exit
R2(config)# interface g0/0
R2(config-if)# ip access-group "BLOCK-LAN1" in
R2(config-if)# ip access-group "BLOCK-LAN2" in
R2(config-if)# exit
R2(config)# interface g0/0
R2(config-if)# no ip access-group in
R2(config-if)# ip access-group "BLOCK-LAN1" in
R2(config-if)# ip access-group "BLOCK-LAN2" in
R2(config-if)# exit
R2(config)# interface g0/0
R2(config-if)# no ip helper-address 10.10.10.1
R2(config-if)# no ip access-group "BLOCK-LAN1" in
R2(config-if)# exit
R2(config)# router ospf 10
R2(config-router)# no passive-interface g0/0
R2(config-router)# passive-interface g0/0.20
R2(config-router)# exit
R2(config)# interface g0/0.20
R2(config-subif)# description "DEFAULT-GATEWAY per LAN-1"
R2(config-subif)# encapsulation dot1q 20
R2(config-subif)# ip address 192.168.20.1 255.255.255.0
R2(config-subif)# ip helper-address 10.10.10.1
R2(config-subif)# ip access-group "BLOCK-LAN1"
R2(config-subif)# duplex auto
R2(config-subif)# speed auto
R2(config-subif)# exit
R2(config)# interface g0/0.88
R2(config-subif)# description "NATIVE VLAN"
R2(config-subif)# encapsulation dot1q 88 native
R2(config-subif)# exit
R2(config)# interface g0/0.99
R2(config-subif)# description "DEFAULT-GATEWAY per MANAGEMENT"
R2(config-subif)# encapsulation dot1q 99
R2(config-subif)# ip address 192.168.99.1 255.255.255.0
R2(config-subif)# ip ospf 10 area 0
R2(config-subif)# exit
R2(config)# router ospf 10
```

```
R2(config-router)# passive-interface g0/0.20
R2(config-router)# passive-interface g0/0.99
R2(config-router)# no passive-interface g0/0
R2(config-router)# exit
R2(config)# interface g0/1
R2(config-if)# no ip helper-address 10.10.10.1
R2(config-if)# no ip access-group "BLOCK-LAN1" in
R2(config-if)# no ip access-group "BLOCK-LAN2" in
R2(config-if)# exit
R2(config)# interface g0/1.24
R2(config-subif)# description "DEFAULT-GATEWAY per LAN-2"
R2(config-subif)# encapsulation dot1q 24
R2(config-subif)# ip address 192.168.24.1 255.255.255.0
R2(config-subif)# ip helper-address 10.10.10.1
R2(config-subif)# ip access-group "BLOCK-LAN2" in
R2(config-subif)# exit
R2(config)# interface g0/1.88
R2(config-subif)# description "NATIVE VLAN"
R2(config-subif)# encapsulation dot1q 88 native
R2(config-subif)# exit
R2(config)# interface g0/1.92
R2(config-subif)# description "DEFAULT-GATEWAY per MANAGEMENT"
R2(config-subif)# encapsulation dot1q 92
R2(config-subif)# ip address 192.168.92.1 255.255.255.0
R2(config-subif)# ip helper-address 10.10.10.1
R2(config-subif)# exit
R2(config)# router ospf 10
R2(config-router)# no passive interface g0/1
R2(config-router)# passive interface g0/1.24
R2(config-router)# passive interface g0/1.92
R2(config-router)# exit
R2(config)# interface g0/1.92
R2(config-subif)# ip ospf 10 area 0
R2(config-subif)# exit
R2(config)#
```

ROUTER 3

10.10.11.0/30

Se0/1/1

PC-PT

Fa0

Fa0/1

Fa0/2

Fa0

Gig0/0

Gig0/1

Fa0/3

PC-PT
PC-E

R3

2960

Fa0

LAN-3
192.168.30.0/24

Fa0

PC-PT
PC-F

```
R3(config)# interface g0/0
R3(config-if)# description "DEFAULT-GATEWAY OF LAN-3"
R3(config-if)# ip address 192.168.30.1 255.255.255.0
R3(config-if)# no shutdown
R3(config-if)# ip helper-address 10.10.11.1
R3(config-if)# exit
R3(config)# interface s0/1/1
R3(config-if)# description "LINK TO R1"
R3(config-if)# ip address 10.10.11.2 255.255.255.252
R3(config-if)# no shutdown
R3(config-if)# exit
// OSPF
R3(config)# router ospf 10
R3(config-router)# router-id 3.3.3.3
R3(config-router)# network 10.10.11.0 0.0.0.3 area 0
R3(config-router)# network 192.168.30.0 0.0.0.255 area 0
R3(config-router)# passive-interface g0/0
R3(config-router)# exit
R3(config)# interface s0/1/0
R3(config-if)# ip ospf network point-to-point
R3(config-if)# exit
R3(config)# interface s0/1/1
R3(config-if)# ip ospf network point-to-point
R3(config-if)# exit
R3(config)# router ospf 10
R3(config-router)# default-information originate
R3(config-router)# exit
// ACL
R3(config)# ip access-list extended "BLOCK_PC-E"
R3(config-ext-nacl)# remark "BLOCCO HTTP a PC_E"
R3(config-ext-nacl)# deny tcp host 192.168.30.9 host 198.160.10.10 eq 80 (www)
R3(config-ext-nacl)# permit ip any any
R3(config-ext-nacl)# exit
R3(config)# interface serial0/1/1
R3(config-if)# ip access-group "BLOCK_PC-E" in
R3(config-if)# exit
R3(config)# interface g0/0.30
R3(config-subif)# encapsulation dot1Q 30
R3(config-subif)# description "DEFAULT-GATEWAY OF LAN-3"
R3(config-subif)# ip address 192.168.30.1 255.255.255.0
R3(config-subif)# ip helper-address 10.10.11.1
R3(config-subif)# ip access-group "BLOCK_PC-E"
R3(config)# interface g0/0.93
```

```
R3(config-subif)# encapsulation dot1Q 93
R3(config-subif)# description "DEFAULT-GATEWAY OF MANAGEMENT"
R3(config-subif)# ip address 192.168.93.1 255.255.255.0
R3(config-subif)# router ospf 10 area 0
R3(config)# interface g0/0.88
R3(config-subif)# description "NATIVE VLAN"
R3(config-subif)# encapsulation dot1Q 88 native
R3(config)# router ospf 10
R3(config-router)# no passive-interface g0/0
R3(config-router)# passive-interface g0/0.30
R3(config-router)# passive-interface g0/0.93
R3(config-router)# exit
R3(config)# interface g0/0
R3(config-if)# ip helper-address 10.10.11.1
R3(config-if)# ip access-group PC_E_FILTERS in
R3(config-if)# exit
R3(config)#
```

ROUTER ISP INTERNET

```
ISP(config)# interface s0/0/0
ISP(config-if)# description "LINK TO R1"
ISP(config-if)# ip address 209.86.120.86 255.255.255.252
ISP(config-if)# no shutdown
ISP(config-if)# exit
ISP(config)# ip route 0.0.0.0 0.0.0.0 s0/0/0
ISP(config)# line console 0
ISP(config-line)# logging synchronous
ISP(config-line)# exit
ISP(config)#
```

209.86.120.84/30

Se0/0/0

ISP

Gig0/0

Se0/0/0

Se0/1/0
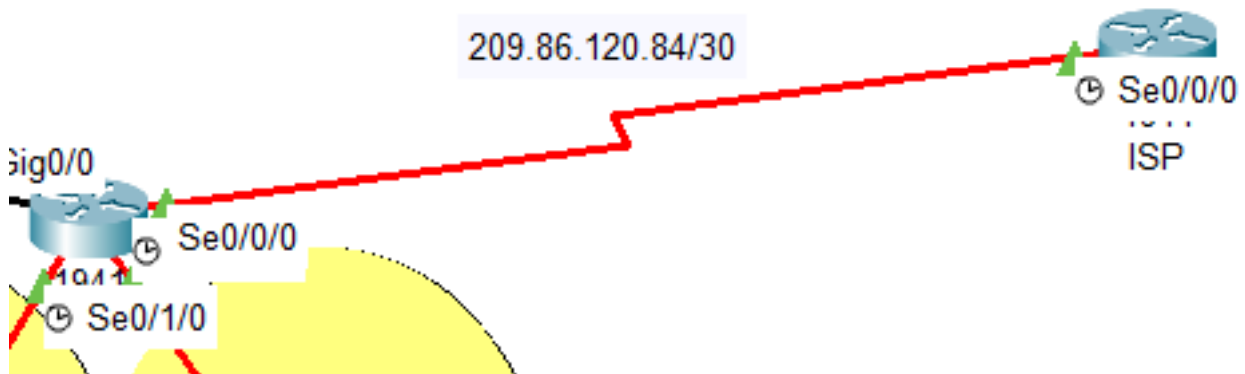
SWITCH 1

```
S1(config)# vlan 20
S1(config-vlan)# name "GARAGE"
S1(config-vlan)# exit
S1(config)# vlan 88
S1(config-vlan)# name "NATIVA"
S1(config-vlan)# exit
S1(config)# vlan 99
S1(config-vlan)# name "MANAGEMENT"
S1(config-vlan)# exit
S1(config)# vlan 999
S1(config-vlan)# name "BLACK_HOLE"
S1(config-vlan)# exit
S1(config)# interface range f0/1-2
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 20
S1(config-if-range)# exit
S1(config)# interface g0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk allowed vlan 20,88,99
S1(config-if)# switchport trunk native vlan 88
S1(config-if)# switchport nonegotiate
S1(config-if)# exit
S1(config)# interface range f0/3-24, g0/2
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 999
S1(config-if-range)# shutdown
S1(config-if-range)# exit
S1(config)# ip default-gateway 192.168.99.1
S1(config-if)# interface vlan 99
S1(config-if)# ip address 192.168.99.5 255.255.255.0
S1(config-if)# exit
// SSH
S1(config)# ip domain-name "cisco.com"
S1(config)# enable secret "cisco"
S1(config)# username admin secret cisco
S1(config)# crypto key generate rsa generate_modulus 1024
S1(config)# line vty 0 15
S1(config-line)# transport input ssh
S1(config-line)# login local
S1(config-line)# exit
S1(config)# ip ssh version 2
S1(config)#
```

SWITCH 2

```
S2(config)# vlan 24
S2(config-vlan)# name "GARAGE"
S2(config-vlan)# exit
S2(config)# vlan 88
S2(config-vlan)# name "NATIVA"
S2(config-vlan)# exit
S2(config)# vlan 92
S2(config-vlan)# name "MANAGEMENT"
S2(config-vlan)# exit
S2(config)# vlan 999
S2(config-vlan)# name "BLACK-HOLE"
S2(config-vlan)# exit
S2(config)# ip default-gateway 192.168.92.1
S2(config)# interface range f0/1-2
S2(config-if-range)# switchport mode access
S2(config-if-range)# switchport access vlan 10
S2(config-if-range)# exit
S2(config)# interface g0/1
S2(config-if)# switchport mode trunk
S2(config-if)# switchport trunk allowed vlan 24,88,92
S2(config-if)# switchport trunk native vlan 88
S2(config-if)# switchport nonegotiate
S2(config-if)# exit
S2(config)# interface range f0/3-24, g0/2
S2(config-if-range)# switchport mode access
S2(config-if-range)# switchport access vlan 999
S2(config-if-range)# shutdown
S2(config-if-range)# exit
S2(config)# ip default-gateway 192.168.92.1
S2(config)# interface vlan 92
S2(config-if)# ip address 192.168.92.5 255.255.255.0
S2(config-if)# exit
S2(config)# interface f0/1
S2(config-if)# swichport mode access
S2(config-if)# swichport access vlan 24
S2(config-if)# exit
S2(config)# interface g0/1
S2(config-if)# switchport trunk native vlan 88
S2(config-if)# switchport mode trunk
S2(config-if)# switchport trunk allowed vlan 24,88,92
S2(config-if)# switchport nonegotiate
S2(config-if)# exit
S2(config)#
```

SWITCH 3

```
S3(config)# vlan 30
S3(config-vlan)# name "HR"
S3(config-vlan)# exit
S3(config)# vlan 88
S3(config-vlan)# name "NATIVA"
S3(config-vlan)# exit
S3(config)# vlan 93
S3(config-vlan)# name "MANAGEMENT"
S3(config-vlan)# exit
S3(config)# vlan 999
S3(config-vlan)# name "BLACK-HOLE"
S3(config-vlan)# exit
S3(config)# interface range f0/1-3
S3(config-if-range)# switchport mode access
S3(config-if-range)# switchport access vlan 30
S3(config-if-range)# exit
S3(config)# interface range f0/4-24, g0/2
S3(config-if-range)# switchport mode access
S3(config-if-range)# switchport access vlan 999
S3(config-if-range)# shutdown
S3(config-if-range)# exit
S3(config)# interface vlan 93
S3(config-if)# ip address 192.168.93.5 255.255.255.0
S3(config-if)# exit
S3(config)# ip default-gateway 192.168.93.1
S3(config)# interface g0/1
S3(config-if)# switchport mode trunk
S3(config-if)# switchport trunk allowed vlan 30,88,93
S3(config-if)# switchport trunk native vlan 88
S3(config-if)# switchport nonegotiate
S3(config-if)# exit
// SSH
S3(config)# ip domain-name "cisco.com"
S3(config)# enable secret "cisco"
S3(config)# username admin secret cisco
S3(config)# crypto key generate rsa generate_modulus 1024
S3(config)# line vty 0 15
S3(config-line)# transport input ssh
S3(config-line)# login local
S3(config-line)# exit
S3(config)# ip ssh version 2
S3(config)#
```