PRUEBA DE HABILIDADES PRÁCTICAS CCNA

WILMAN AUGUSTO CASTAÑEDA GONZALEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGIA E INGENIERIA

DIPLOMADO DE PROFUNDIZACION CISCO CCNA

FACATATIVÁ

2018

PRUEBA DE HABILIDADES PRÁCTICAS CCNA

WILMAN AUGUSTO CASTAÑEDA GONZALEZ

Trabajo final de grado

Tutor de Curso

Efraín Alejandro Pérez

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGIA E INGENIERIA

DIPLOMADO DE PROFUNDIZACION CISCO CCNA

FACATATIVA

2018

TABLA DE CONTENIDO

INTRODUCCION....6

1. ESCENARIO PROPUESTO....7

1.1 ESCENARIO....7

1.2 TOPOLOGIA DE RED....7

1.2.1 Configurar el protocolo de enrutamiento OSPFv2 bajo los siguientes criterios:....9

2. VERIFICAR INFORMACION DE OSPF....9

2.1 TABLAS DE ENRUTAMIENTO....9

2.1.1 Visuaizar tablas de enrutamiento y routers conectados por OSPF v2....9

2.2 LISTAS RESUMIDAS....10

3. CONFIGURAR VLANS....11

3.1 Configurar VLANs, Puertos troncales, puertos de acceso, encapsulamiento, Inter-VLAN Routing y Seguridad en los Switches acorde a la topología de red establecida.....11

4. DESHABILITAR DNS LOOKUP EN S3....15

5. ASIGNACION IP A LOS SWITCHES....16

6. DESACTIVAR INTERFACES INUTILIZADAS EN LA RED (COMANDO SHUTDOWN)....17

7. RESERVAR LAS PRIMERAS 30 DIRECCIONES IP DE LAS VLAN 30 Y 40 PARA CONFIGURACIONES ESTÁTICAS.....17

8. CONFIGURAR NAT EN R2 PARA PERMITIR QUE LOS HOST PUEDAN SALIR A INTERNET....20

9. CONFIGURAR AL MENOS DOS LISTAS DE ACCESO DE TIPO ESTANDAR A SU CRITERIO PARA RESTRINGIR O PERMITIR TRÁFICO DESDE R1 O R3 HACIA R2....26

10. CONFIGURAR AL MENOS DOS LISTAS DE ACCESO DE TIPO EXTENDIDO O NOMBRADAS A SU CRITERIO PARA RESTRINGIR O PERMITIR TRÁFICO DESDE R1 O R3 HACIA R2....29

11. VERIFICAR PROCESOS DE COMUNICACIÓN Y REDIRECCIONAMIENTO DE TRÁFICO EN LOS ROUTERS MEDIANTE EL USO DE PING Y TRACEROUTE....30

BIBLIOGRAFIA....33

GLOSARIO

VLAN. Crea un dominio de difusión lógico que puede abarcar varios segmentos, proporcionando una manera de agrupar dispositivos de una red LAN.

TOPOLOGÍA. Existe la topología física y lógica. La primera, es la forma como los dispositivos de red se interconectan. La segunda, es la ruta por la cual se transfieren los datos en una red

ENRUTAMIENTO. En una red de datos, es el proceso de transferir información a través de una internetwork de origen a destino.

ENRUTAMIENTO ESTATICO. Cuando las redes remotas se introducen de forma manual en la tabla de rutas.

ENRUTAMIENTO DINÁMICO. Las rutas remotas se descubren de forma automática mediante un protocolo de routing dinámico.

LISTAS DE CONTROL DE ACCESO. Es una lista secuencial de instrucciones Permit o Deny que se aplican a los protocolos de capa superior o a las direcciones para controlar el tráfico desde y hacia la red.

DHCP. Es un protocolo de configuración dinámica de host que simplifica la asignación de direcciones IP tanto de equipos de escritorio como de dispositivos móviles.

NAT. Traducción de direcciones de red. Es un mecanismo utilizado por los routers de red para traducir la dirección ipv4 interna del dispositivo a una dirección pública del conjunto de NAT.

RESUMEN

Actualmente, las compañías necesitan tener acceso instantáneo de red desde y hacia cualquier parte del mundo y en cualquier momento. Por ende, para acceder a las redes de internetworking, no solo se requiere la implementación de tecnología de acceso, sino también tecnologías que permitan el intercambio de recursos en tiempo real, manteniendo la seguridad en la red y la convergencia de la misma. Los dispositivos intermediarios (switch, router, etc) son los que permiten el acceso a la red de los dispositivos finales (host, servidores, etc), proporcionando una conexión rápida, segura y confiable entre los host.

El objetivo de este trabajo es diseñar un escenario de red que permita conjugar los recursos de red y las tecnologías de acceso a ésta, a través de la configuración física y lógica tanto de dispositivos finales como intermediarios, permitiendo verificar el flujo de tráfico y el funcionamiento de los servicios avanzados de red. Bajo este contexto, el administrador deberá establecer los parámetros de direccionamiento IP, protocolos de enrutamiento, redes de área local virtuales, listas de control de acceso, DHCP y servicios NAT

INTRODUCCION

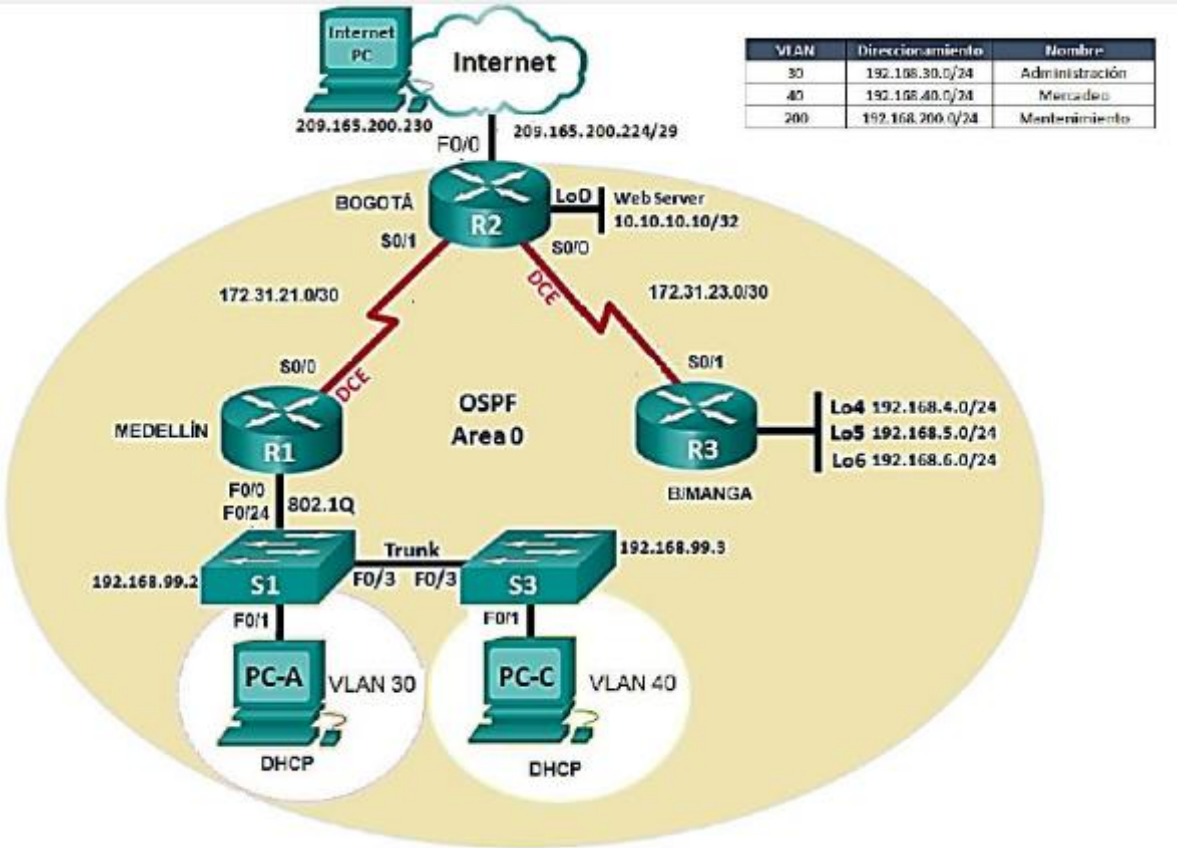
En el presente trabajo, se expondrá acerca de un estudio de caso donde el usuario deberá interconectar a través del software Packet Tracer, una serie de dispositivos que conformarán una red virtual organizativa y configurar una serie de parámetros para esta red tales como direccionamiento IP, protocolos de enrutamiento, configuración de VLANs, listas de control de acceso, DHCP y NAT. Adicionalmente, el administrador de la red deberá hacer pruebas de configuración de red, usando la visualización de tablas de enrutamiento, listas resumidas, costo de interfaces, entre otras y verificación de procesos de comunicación usando los comandos PING y TRACEROUTE.

1. ESCENARIO PROPUESTO

1.1 ESCENARIO

Una empresa de Tecnología posee tres sucursales distribuidas en las ciudades de Bogotá, Medellín y Bucaramanga, en donde el estudiante será el administrador de la red, el cual deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red.

1.2 TOPOLOGIA DE RED



VLAN	Direccionamiento	Nombre
30	192.168.30.0/24	Administración
40	192.168.40.0/24	Mercadeo
200	192.168.200.0/24	Mantenimiento

Configurar el direccionamiento IP acorde con la topología de red para cada uno de los dispositivos que forman parte del escenario

```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, 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

     10.0.0.0/29 is subnetted, 1 subnets
C       10.10.10.8 is directly connected, FastEthernet0/1
     172.31.0.0/30 is subnetted, 2 subnets
C       172.31.21.0 is directly connected, Serial0/0/1
C       172.31.23.0 is directly connected, Serial0/0/0
C    192.168.7.0/24 is directly connected, FastEthernet0/0
```

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, 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

     172.31.0.0/30 is subnetted, 1 subnets
C       172.31.21.0 is directly connected, Serial0/0/0
C    192.168.30.0/24 is directly connected, FastEthernet0/0.30
C    192.168.40.0/24 is directly connected, FastEthernet0/0.40
C    192.168.200.0/24 is directly connected, FastEthernet0/0.200
```

```
R3#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

     172.31.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.31.23.0/30 is directly connected, Serial0/0/1
L       172.31.23.2/32 is directly connected, Serial0/0/1
     192.168.4.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.4.0/24 is directly connected, GigabitEthernet0/0
L       192.168.4.1/32 is directly connected, GigabitEthernet0/0
     192.168.5.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.5.0/24 is directly connected, GigabitEthernet0/1
L       192.168.5.1/32 is directly connected, GigabitEthernet0/1
     192.168.6.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.6.0/24 is directly connected, GigabitEthernet0/2
L       192.168.6.1/32 is directly connected, GigabitEthernet0/2
```

1.2.1 Configurar el protocolo de enrutamiento OSPFv2 bajo los siguientes criterios:

OSPFv2 area 0

Configuration Item or Task	Specification
Router ID R1	1.1.1.1
Router ID R2	2.2.2.2
Router ID R3	3.3.3.3
Configurar todas las interfaces LAN como pasivas	
Establecer el ancho de banda para enlaces seriales en	128 Kb/s
Ajustar el costo en la métrica de S0/0 a	7500

Para ajustar el costo de la métrica de los puertos s0/0/0 en 7500, se utiliza el comando ***ip ospf cost 7500*** en el modo de configuración de la interfaz

Para ajustar el ancho de banda de los puertos seriales de todos los routers en 128 kb/s se utiliza el comando ***bandwidth 128*** en el modo de configuración de la interfaz.

2. VERIFICAR INFORMACION DE OSPF

2.1 TABLAS DE ENRUTAMIENTO

2.1.1 Visuaizar tablas de enrutamiento y routers conectados por OSPF v2

```
R2#show ip route ospf
O    192.168.4.0 [110/7501] via 172.31.23.2, 00:17:26, Serial0/0/0
O    192.168.5.0 [110/7501] via 172.31.23.2, 00:17:26, Serial0/0/0
O    192.168.6.0 [110/7501] via 172.31.23.2, 00:17:26, Serial0/0/0
O    192.168.30.0 [110/7501] via 172.31.21.2, 00:09:44, Serial0/0/1
O    192.168.40.0 [110/7501] via 172.31.21.2, 00:09:44, Serial0/0/1
```

```
R1#show ip route ospf
     10.0.0.0/29 is subnetted, 1 subnets
O       10.10.10.8 [110/7501] via 172.31.21.1, 00:15:38, Serial0/0/0
     172.31.0.0/30 is subnetted, 2 subnets
O       172.31.23.0 [110/15000] via 172.31.21.1, 00:15:38, Serial0/0/0
O    192.168.4.0 [110/15001] via 172.31.21.1, 00:15:38, Serial0/0/0
O    192.168.5.0 [110/15001] via 172.31.21.1, 00:15:38, Serial0/0/0
O    192.168.6.0 [110/15001] via 172.31.21.1, 00:15:38, Serial0/0/0
O    192.168.7.0 [110/7501] via 172.31.21.1, 00:15:38, Serial0/0/0
```

```
R3#show ip route ospf
     10.0.0.0/29 is subnetted, 1 subnets
O       10.10.10.8 [110/782] via 172.31.23.1, 00:05:07, Serial0/0/1
     172.31.0.0/16 is variably subnetted, 3 subnets, 2 masks
O       172.31.21.0 [110/8281] via 172.31.23.1, 00:05:07, Serial0/0/1
O    192.168.7.0 [110/782] via 172.31.23.1, 00:05:07, Serial0/0/1
O    192.168.30.0 [110/8282] via 172.31.23.1, 00:05:07, Serial0/0/1
O    192.168.40.0 [110/8282] via 172.31.23.1, 00:05:07, Serial0/0/1
```

2.2 LISTAS RESUMIDAS

Visualizar lista resumida de interfaces por OSPF en donde se ilustre el costo de cada interface

2.3 PROCESOS

Visualizar el OSPF Process ID, Router ID, Address summarizations, Routing Networks, and passive interfaces configuradas en cada router.

```
R2#show ip protocols

Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 2.2.2.2
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.7.0 0.0.0.255 area 0
    172.31.21.0 0.0.0.3 area 0
    172.31.23.0 0.0.0.3 area 0
    10.10.10.8 0.0.0.7 area 0
  Passive Interface(s):
    FastEthernet0/0
    FastEthernet0/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:20:08
    2.2.2.2              110      00:14:54
    3.3.3.3              110      00:08:53
  Distance: (default is 110)
```

```
R3#show ip protocols

Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 3.3.3.3
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.31.23.0 0.0.0.3 area 0
    192.168.4.0 0.0.0.255 area 0
    192.168.5.0 0.0.0.255 area 0
    192.168.6.0 0.0.0.255 area 0
  Passive Interface(s):
    GigabitEthernet0/0
    GigabitEthernet0/1
    GigabitEthernet0/2
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:21:29
    2.2.2.2              110      00:16:15
    3.3.3.3              110      00:10:14
  Distance: (default is 110)
```

```
R1#show ip protocols

Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.31.21.0 0.0.0.3 area 0
    192.168.99.0 0.0.0.255 area 0
    192.168.30.0 0.0.0.255 area 0
    192.168.40.0 0.0.0.255 area 0
  Passive Interface(s):
    FastEthernet0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:22:50
    2.2.2.2              110      00:17:37
    3.3.3.3              110      00:11:35
  Distance: (default is 110)
```

3. CONFIGURAR VLANS

3.1 Configurar VLANs, Puertos troncales, puertos de acceso, encapsulamiento, Inter-VLAN Routing y Seguridad en los Switches acorde a la topología de red establecida.

```
S1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Gig0/1, Gig0/2
30   Administracion                   active    Fa0/1
40   Mercadeo                         active
200  Mantenimiento                    active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

R1#show ip route
Codes: C - connected, S - static, I - IGRP, 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

     10.0.0.0/29 is subnetted, 1 subnets
O       10.10.10.8 [110/7501] via 172.31.21.1, 00:39:43, Serial0/0/0
     172.31.0.0/30 is subnetted, 2 subnets
C       172.31.21.0 is directly connected, Serial0/0/0
O       172.31.23.0 [110/15000] via 172.31.21.1, 00:39:43, Serial0/0/0
O    192.168.4.0/24 [110/15001] via 172.31.21.1, 00:39:43, Serial0/0/0
O    192.168.5.0/24 [110/15001] via 172.31.21.1, 00:39:43, Serial0/0/0
O    192.168.6.0/24 [110/15001] via 172.31.21.1, 00:39:43, Serial0/0/0
O    192.168.7.0/24 [110/7501] via 172.31.21.1, 00:39:43, Serial0/0/0
C    192.168.30.0/24 is directly connected, FastEthernet0/0.30
C    192.168.40.0/24 is directly connected, FastEthernet0/0.40
C    192.168.200.0/24 is directly connected, FastEthernet0/0.200
R1#
```

Ctrl+F6 to exit CLI focus

```
S2#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
30   Administracin                    active
40   Mercadeo                         active    Fa0/1
200  Mantenimiento                    active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

S1#show int f0/24 switchport
Name: Fa0/24
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
```

```
Sl#show int f0/3 sw
Sl#show int f0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dotlq
Operational Trunking Encapsulation: dotlq
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dotlq
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none
```

```
Sl#show int f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dotlq
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 30 (Administracion)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dotlq
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none
```

```
S2#show int f0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none

S2#show int f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 40 (Mercadeo)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none
```

4. DESHABILITAR DNS LOOKUP EN S3

```
S3(config)#no ip domain lookup
S3(config)#end
S3#
%SYS-5-CONFIG_I: Configured from console by console
```

5. ASIGNACION IP A LOS SWITCHES

```
S1#show ip interface vlan 1
Vlan1 is up, line protocol is up
  Internet address is 192.168.99.2/24
  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
  Outgoing access list is not set
  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 disabled
  IP fast switching on the same interface is disabled
  IP Null turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are None
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
```

```
S2#show ip int vlan1
Vlan1 is up, line protocol is up
  Internet address is 192.168.99.3/24
  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
  Outgoing access list is not set
  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 disabled
  IP fast switching on the same interface is disabled
  IP Null turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are None
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
```

6. DESACTIVAR INTERFACES INUTILIZADAS EN LA RED (COMANDO SHUTDOWN)

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/2, Fa0/4, Fa0/5, Fa0/6
                                                 Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                 Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Gig0/1, Gig0/2
30   Administracion                    active    Fa0/1
40   Mercadeo                          active
200  Mantenimiento                     active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

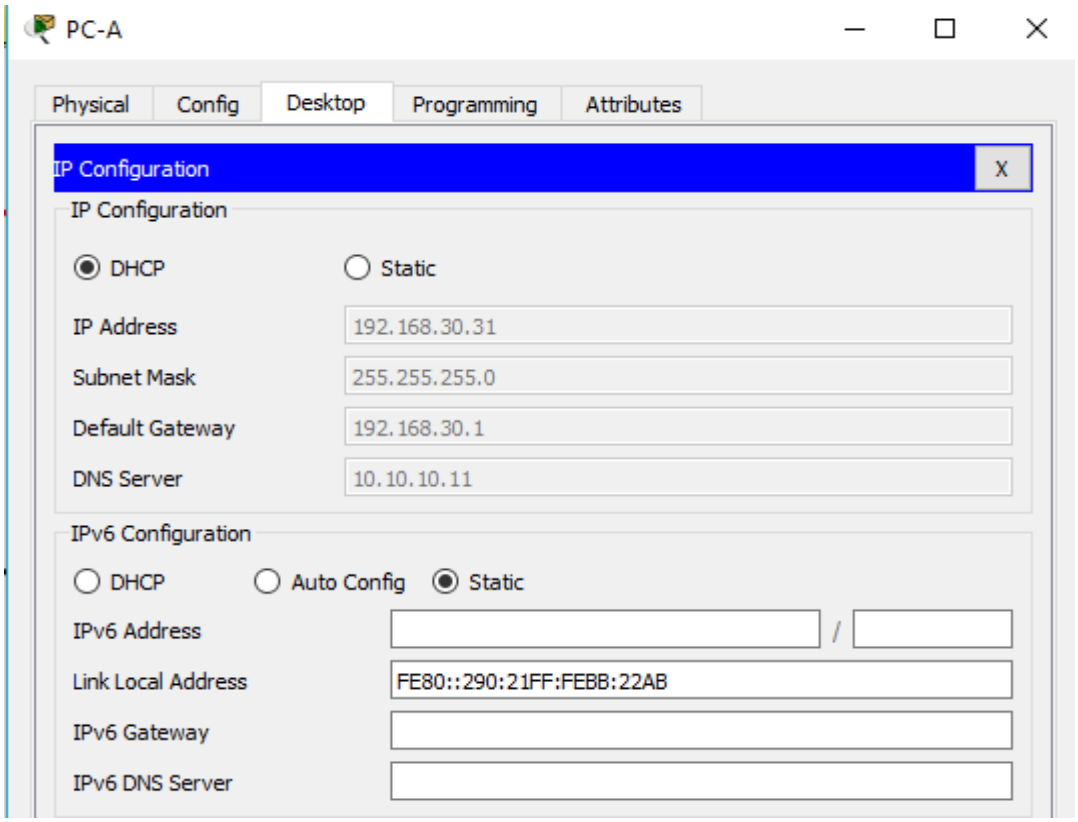
```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/2, Fa0/4, Fa0/5, Fa0/6
                                                 Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                 Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24, Gig0/1, Gig0/2
30   Administracin                     active
40   Mercadeo                          active    Fa0/1
200  Mantenimiento                     active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

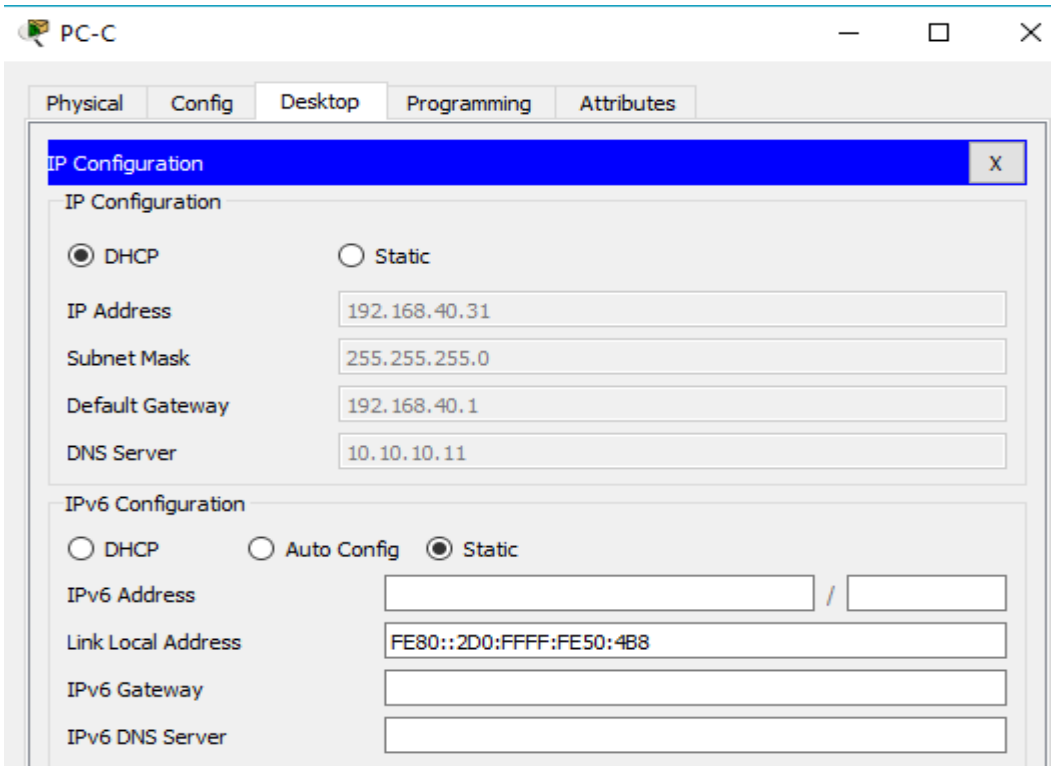
7. RESERVAR LAS PRIMERAS 30 DIRECCIONES IP DE LAS VLAN 30 Y 40 PARA CONFIGURACIONES ESTÁTICAS.

Configurar DHCP pool para VLAN 30	Name: ADMINISTRACION DNS-Server 10.10.10.11 Domain name: ccna-unad.com Establecer default gateway
Configurar DHCP pool para VLAN 40	Name: Mercadeo DNS-Server 10.10.10.11 Domain name: ccna-unad.com Establecer default gateway

```
R1#show ip dhcp pool

Pool ADMINISTRACION :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 1
 Excluded addresses             : 4
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 192.168.30.1         192.168.30.1     - 192.168.30.254    1    / 4     / 254

Pool MERCADEO :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 1
 Excluded addresses             : 4
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 192.168.40.1         192.168.40.1     - 192.168.40.254    1    / 4     / 254
```

```
R1#show running-config
Building configuration...

Current configuration : 1682 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R1
!
!
!
!
ip dhcp excluded-address 192.168.30.1 192.168.30.30
ip dhcp excluded-address 192.168.30.254
ip dhcp excluded-address 192.168.40.1 192.168.40.30
ip dhcp excluded-address 192.168.40.254
!
ip dhcp pool ADMINISTRACION
 network 192.168.30.0 255.255.255.0
 default-router 192.168.30.1
 dns-server 10.10.10.11
ip dhcp pool MERCADEO
 network 192.168.40.0 255.255.255.0
 default-router 192.168.40.1
 dns-server 10.10.10.11
```


PC-A
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
192.168.30.31
Subnet Mask
255.255.255.0
Default Gateway
192.168.30.1
DNS Server
10.10.10.11
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::290:21FF:FEBB:22AB
IPv6 Gateway
IPv6 DNS Server

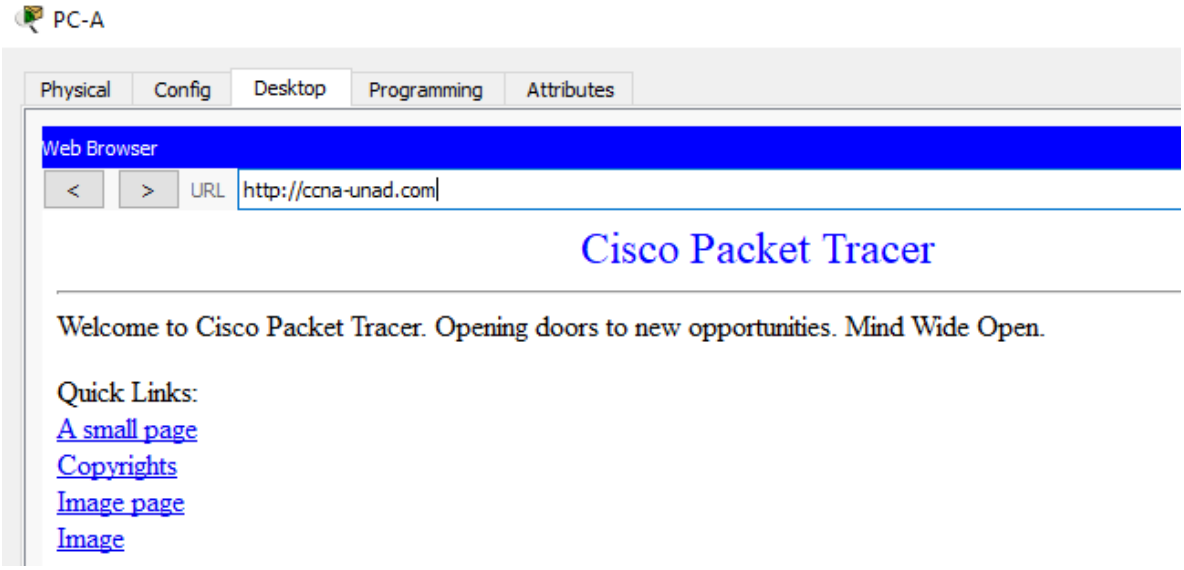

PC-C
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
192.168.40.31
Subnet Mask
255.255.255.0
Default Gateway
192.168.40.1
DNS Server
10.10.10.11
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::2D0:FFFF:FE50:4B8
IPv6 Gateway
IPv6 DNS Server

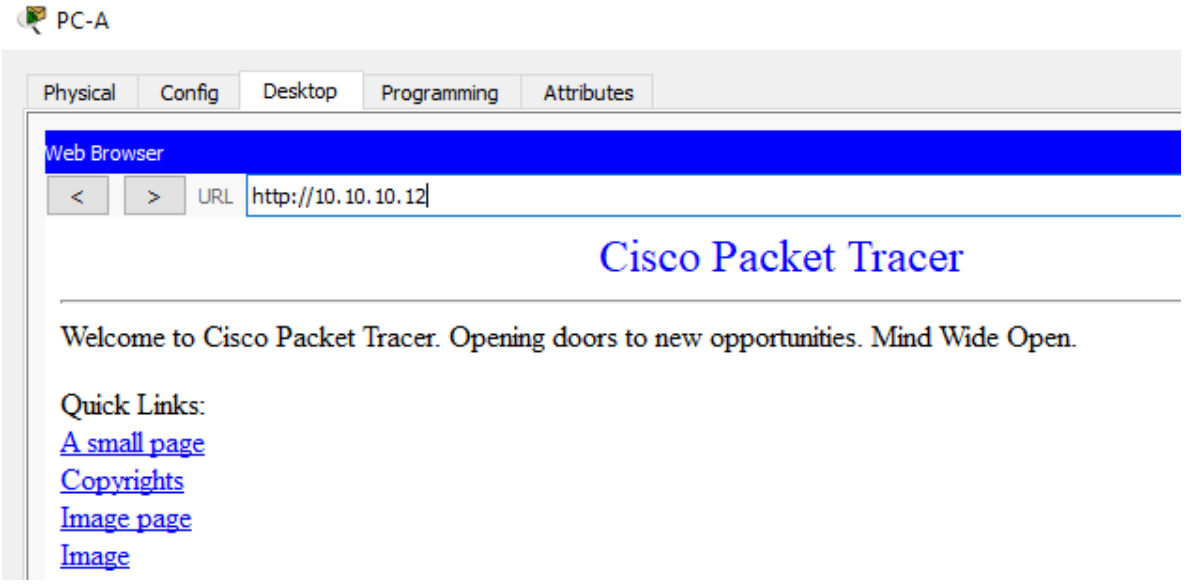
8. CONFIGURAR NAT EN R2 PARA PERMITIR QUE LOS HOST PUEDAN SALIR A INTERNET

La dirección ip actual del servidor es ***10.10.10.12/29*** y la dirección web actual es **ccna-unad.com**

Como está configurado el router ospf, se puede acceder a la web desde cualquier equipo. Veamos:

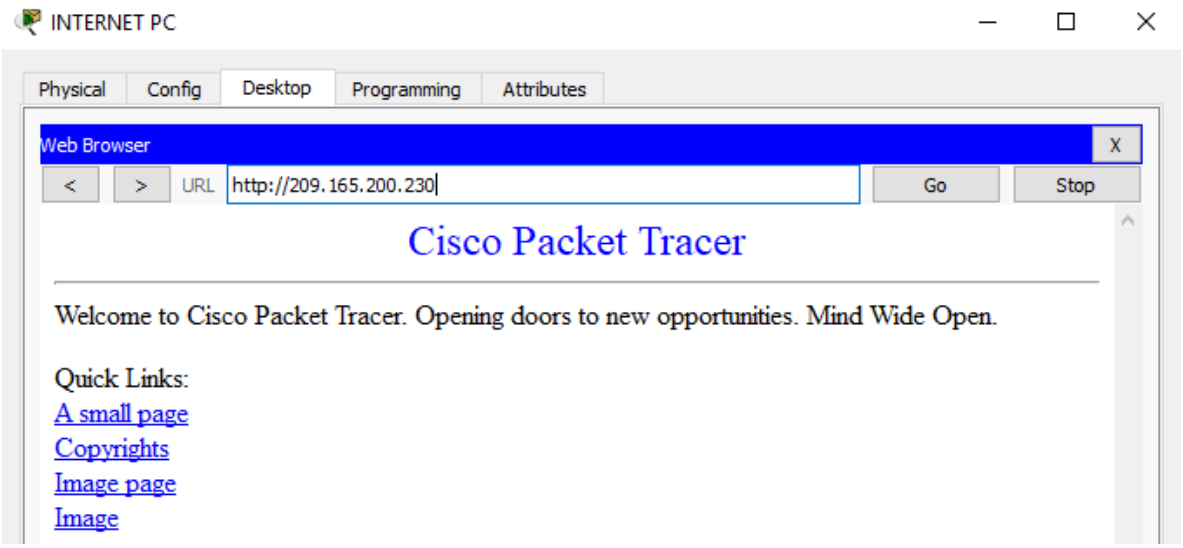
Desde PC-A





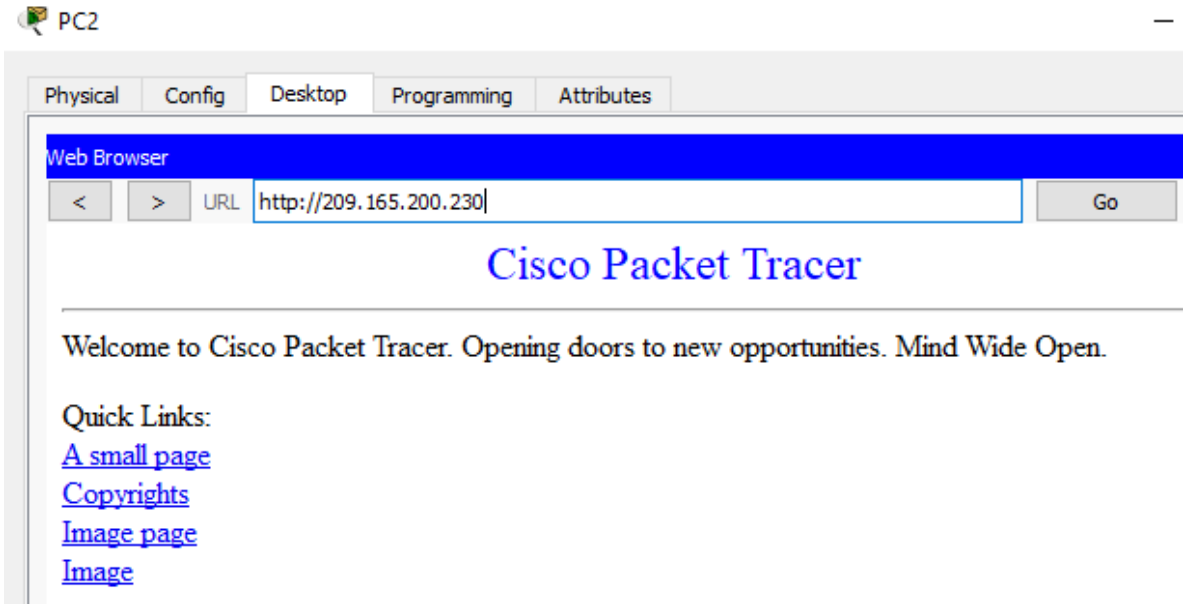
Ahora, se va a configurar NAT estática para que el R2 traduzca la dirección ip privada del servidor web **10.10.10.12** en la dirección ip pública **209.165.200.230**

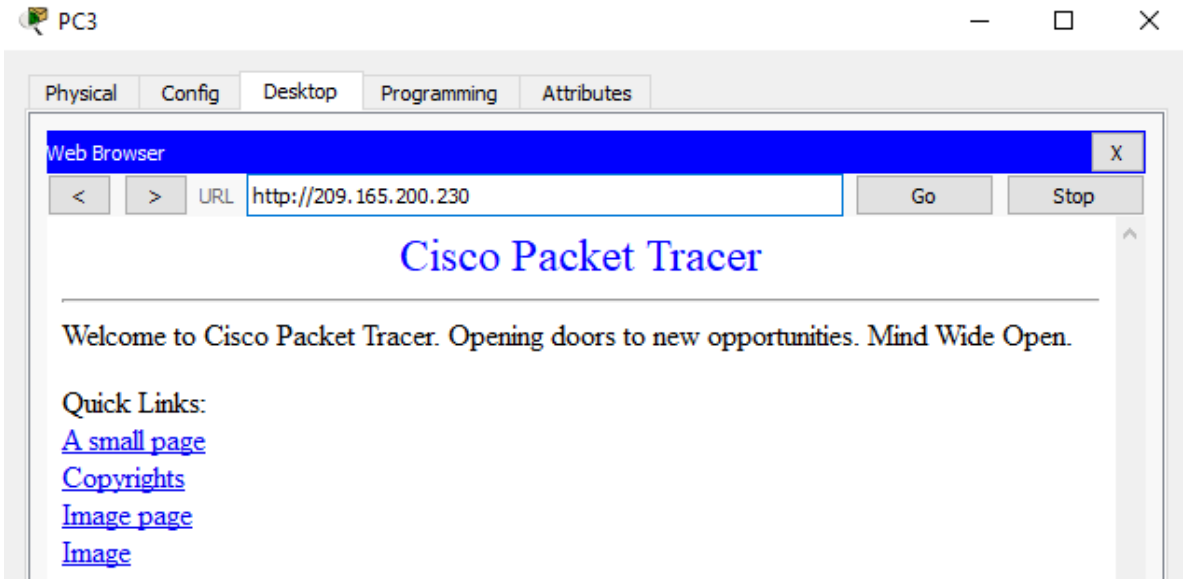
```
R2(config)#ip nat inside source static 10.10.10.12
209.165.200.230
R2(config)#nt f0/0
           ^
% Invalid input detected at '^' marker.

R2(config)#int f0/0
R2(config-if)#ip add
R2(config-if)#ip address 192.168.7.1 255.255.255.0
R2(config-if)#ip na
R2(config-if)#ip nat o
R2(config-if)#ip nat outside
R2(config-if)#exit
R2(config)#int f0/1
R2(config-if)#ip add
R2(config-if)#ip address 10.10.10.13 255.255.255.248
R2(config-if)#ip na
R2(config-if)#ip nat in
R2(config-if)#ip nat inside
R2(config-if)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

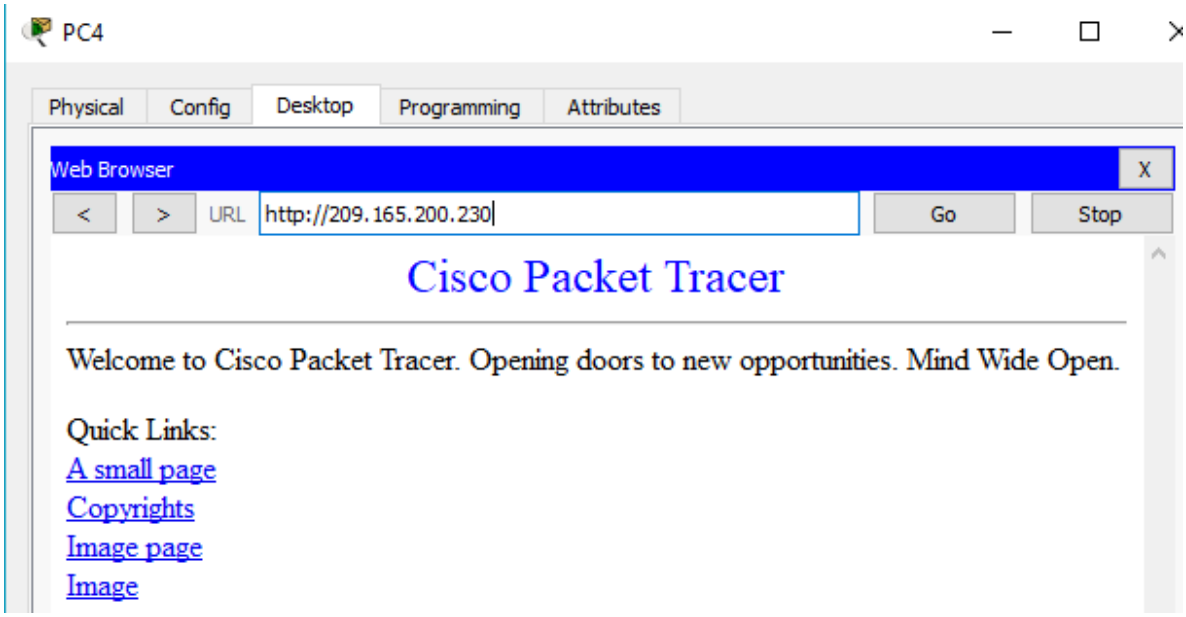


Ahora, se va a configurar para que pueda traducir las demás ip privadas de los demás host que corresponde a las otras redes:

```
R3(config)#ip nat inside source static 10.10.10.12 209.165.200.230
R3(config)#int s0/0/1
R3(config-if)#ip add
R3(config-if)#ip address 172.31.23.2 255.255.255.252
R3(config-if)#ip nat ins
R3(config-if)#ip nat inside
R3(config-if)#exit
R3(config)#int g0/0
R3(config-if)#ip add
R3(config-if)#ip address 192.168.4.1 255.255.255.0
R3(config-if)#ip nat ou
R3(config-if)#ip nat outside
R3(config-if)#exit
R3(config)#int g0/1
R3(config-if)#ip add
R3(config-if)#ip address 192.168.5.1 255.255.255.0
R3(config-if)#ip nat o
R3(config-if)#ip nat outside
R3(config-if)#exit
R3(config)#int g0/2
R3(config-if)#ip add
R3(config-if)#ip address 192.168.6.1 255.255.255.0
R3(config-if)#exit
R3(config)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console
```

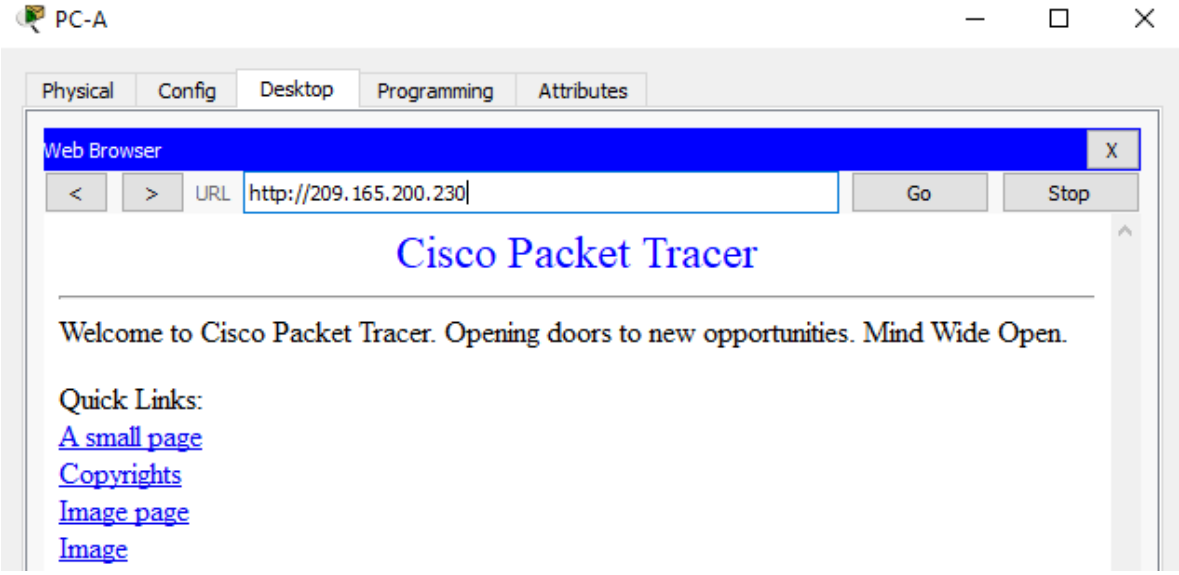




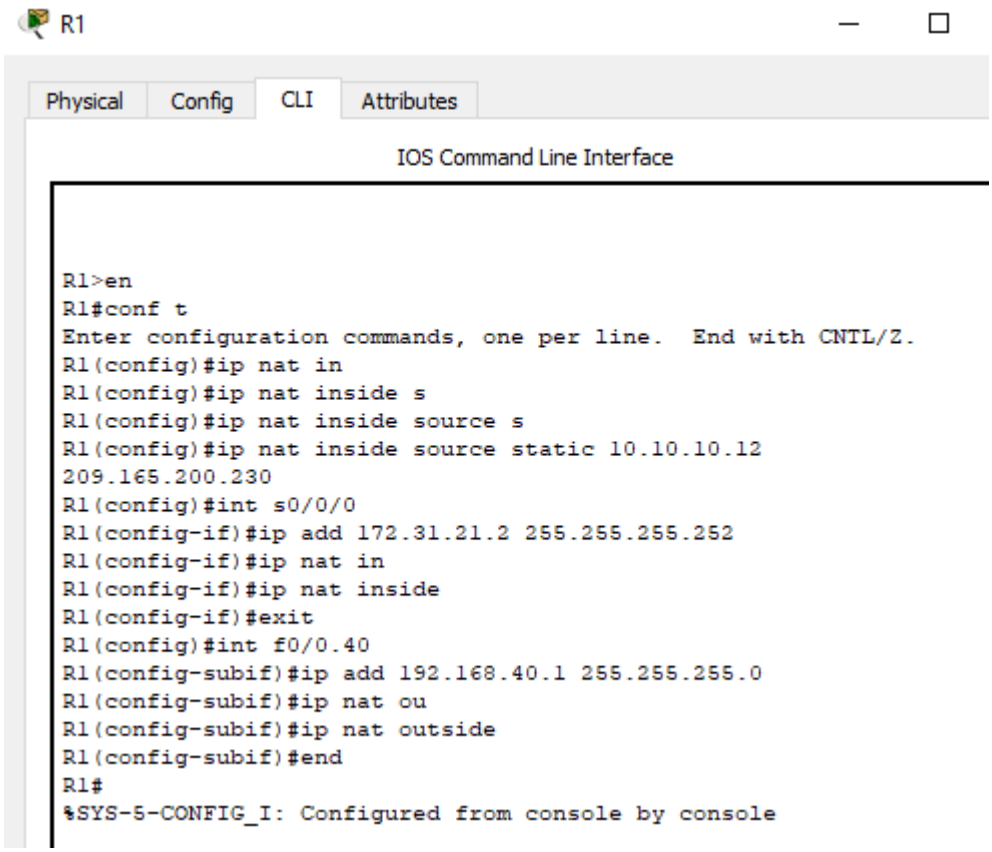


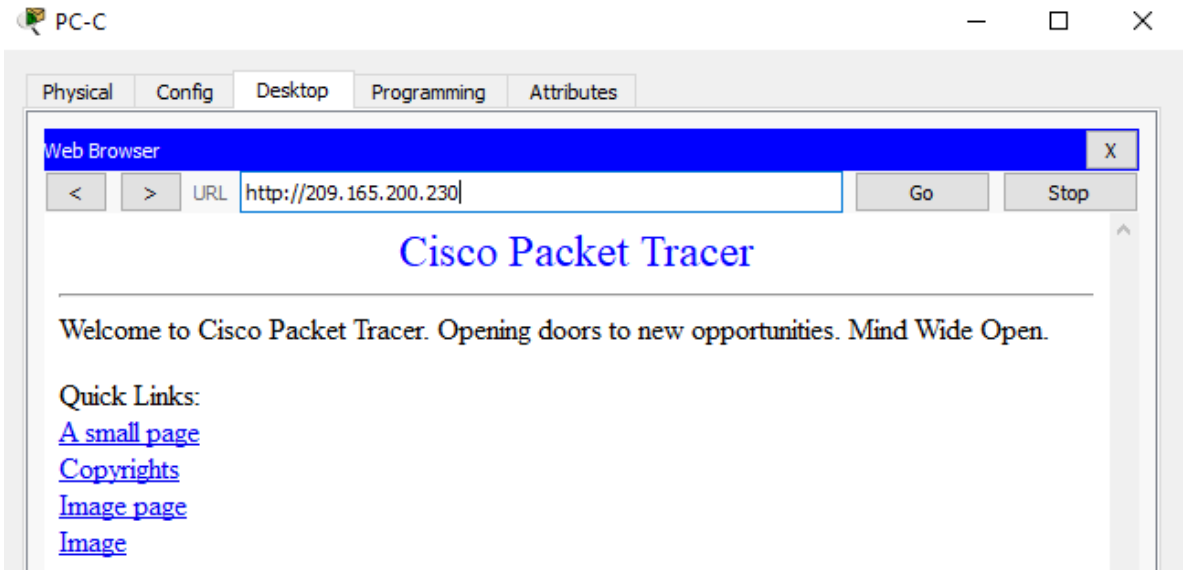
Ahora, se va a configurar el R1 para que pueda traducir la dirección ip privada del servidor en la dirección ip pública **209.165.200.230** desde el pc de la vlan 30 cuando acceda a la pagina web:

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip nat ins
R1(config)#ip nat inside so
R1(config)#ip nat inside source s
R1(config)#ip nat inside source static 10.10.10.12 209.165.200.230
R1(config)#int s0/0/0
R1(config-if)#ip add
R1(config-if)#ip address 172.31.21.2 255.255.255.252
R1(config-if)#ip na
R1(config-if)#ip nat in
R1(config-if)#ip nat inside
R1(config-if)#exit
R1(config)#int f0/0
R1(config-if)#ip add 192.168.30.1 255.255.255.0
% 192.168.30.0 overlaps with FastEthernet0/0.30
R1(config-if)#int f0/0.30
R1(config-subif)#ip ad
R1(config-subif)#ip address 192.168.30.1 255.255.255.0
R1(config-subif)#ip n
R1(config-subif)#ip nat ou
R1(config-subif)#ip nat outside
R1(config-subif)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```



Por último, se lleva a cabo este mismo paso, pero con la VLAN 40:





Se verifica la tabla NAT de todos los routers presentes en la red

```
R1#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  209.165.200.230   10.10.10.12        ---                ---
tcp 209.165.200.230:80 10.10.10.12:80     192.168.30.31:1026 192.168.30.31:1026
tcp 209.165.200.230:80 10.10.10.12:80     192.168.30.31:1027 192.168.30.31:1027
tcp 209.165.200.230:80 10.10.10.12:80     192.168.40.31:1025 192.168.40.31:1025

R3#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  209.165.200.230   10.10.10.12        ---                ---
tcp 209.165.200.230:80 10.10.10.12:80     192.168.4.10:1025  192.168.4.10:1025
tcp 209.165.200.230:80 10.10.10.12:80     192.168.4.10:1026  192.168.4.10:1026
tcp 209.165.200.230:80 10.10.10.12:80     192.168.5.10:1025  192.168.5.10:1025
tcp 209.165.200.230:80 10.10.10.12:80     192.168.6.10:1025  192.168.6.10:1025
tcp 209.165.200.230:80 10.10.10.12:80     192.168.6.10:1026  192.168.6.10:1026

R2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  209.165.200.230   10.10.10.12        ---                ---
tcp 209.165.200.230:80 10.10.10.12:80     192.168.4.10:1025  192.168.4.10:1025
tcp 209.165.200.230:80 10.10.10.12:80     192.168.4.10:1026  192.168.4.10:1026
tcp 209.165.200.230:80 10.10.10.12:80     192.168.5.10:1025  192.168.5.10:1025
tcp 209.165.200.230:80 10.10.10.12:80     192.168.6.10:1025  192.168.6.10:1025
tcp 209.165.200.230:80 10.10.10.12:80     192.168.6.10:1026  192.168.6.10:1026
```

En ese orden de ideas, se puede acceder a la página web utilizando la dirección IP pública ***209.165.200.230***

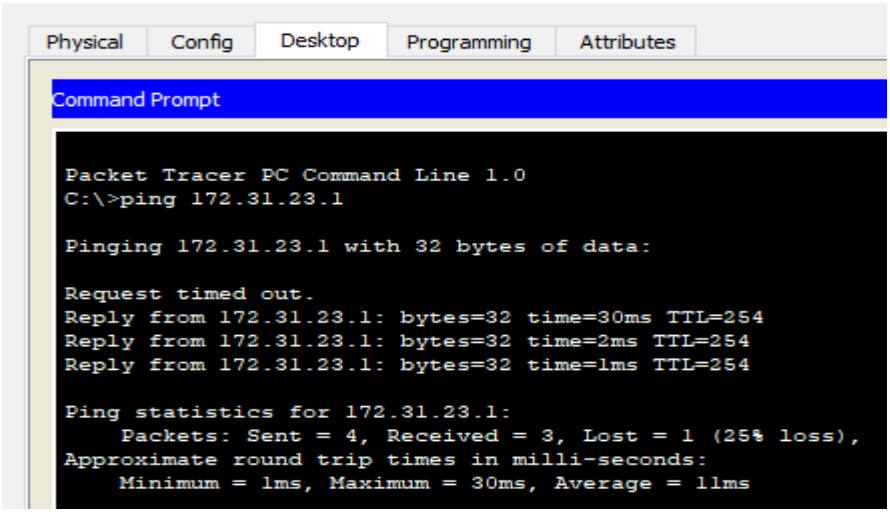
9. CONFIGURAR AL MENOS DOS LISTAS DE ACCESO DE TIPO ESTANDAR A SU CRITERIO PARA RESTRINGIR O PERMITIR TRÁFICO DESDE R1 O R3 HACIA R2

En este caso, se va a configurar dos listas de acceso de la siguiente manera:

- La primera, va denegar el tráfico de la dirección ip del PC-3 hasta el R2.
- La segunda, va denegar el tráfico de la dirección ip del PC-4 hasta el R2.

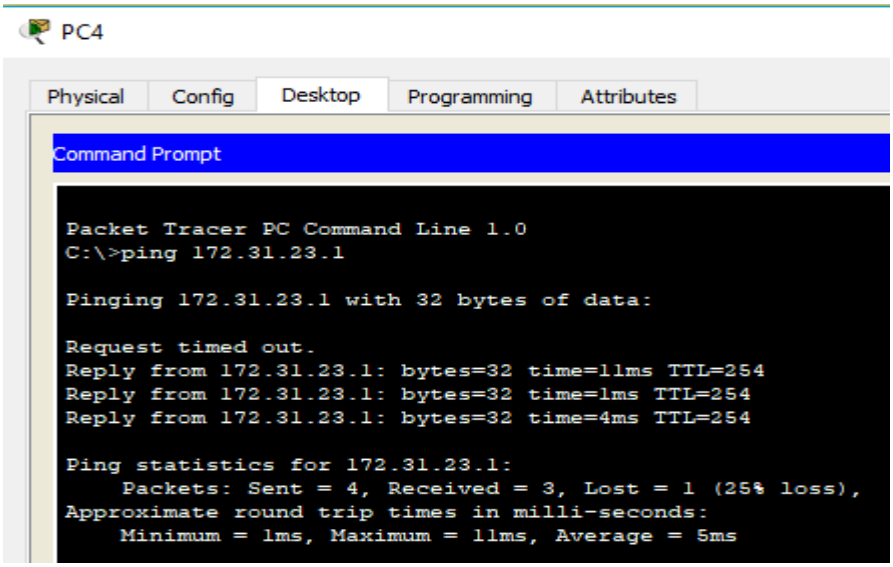
Primero, veamos el ping en el PC-3 hacia el R2

PC3



Luego, se hace ping en el PC-4 hacia el R2

PC4



Denegación tráfico de la PC-3 hacia el R2

```
R3(config)#access-list 1 deny host 192.168.5.10
R3(config)#acc
R3(config)#access-list 1 per
R3(config)#access-list 1 permit a
R3(config)#access-list 1 permit any
R3(config)#int s0/0/1
R3(config-if)#ip acc
R3(config-if)#ip access-group 1 o
R3(config-if)#ip access-group 1 out
R3(config-if)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console
```

Verificación de denegación de tráfico en la PC-3 hacia el R2

```
C:\>ping 172.31.23.1

Pinging 172.31.23.1 with 32 bytes of data:

Reply from 192.168.5.1: Destination host unreachable.
Reply from 192.168.5.1: Destination host unreachable.
Reply from 192.168.5.1: Destination host unreachable.
Reply from 192.168.5.1: Destination host unreachable.

Ping statistics for 172.31.23.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Ahora se configura la denegación de tráfico de la PC-4 hacia el R2 con otra lista de control de acceso:

```
R3(config)#access-list 2 deny host 192.168.6.10
R3(config)#acc
R3(config)#access-list 2 pe
R3(config)#access-list 2 permit a
R3(config)#access-list 2 permit any
R3(config)#int s0/0/1
R3(config-if)#ip acc
R3(config-if)#ip access-group 2 o
R3(config-if)#ip access-group 2 out
R3(config-if)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console
```

Verificación de denegación de tráfico en la PC-4 hacia el R2

```
C:\>ping 172.31.23.1

Pinging 172.31.23.1 with 32 bytes of data:

Reply from 192.168.6.1: Destination host unreachable.
Reply from 192.168.6.1: Destination host unreachable.
Reply from 192.168.6.1: Destination host unreachable.
Reply from 192.168.6.1: Destination host unreachable.

Ping statistics for 172.31.23.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Verificación de las listas de acceso

```
R3#show access-lists
Standard IP access list 1
    10 deny host 192.168.5.10 (4 match(es))
    20 permit any
Standard IP access list 2
    10 deny host 192.168.6.10 (24 match(es))
    20 permit any (9 match(es))
```

10. CONFIGURAR AL MENOS DOS LISTAS DE ACCESO DE TIPO EXTENDIDO O NOMBRADAS A SU CRITERIO PARA RESTRINGIR O PERMITIR TRÁFICO DESDE R1 O R3 HACIA R2

En la primera lista extendida (ACL1), se va a denegar tráfico ICMP de la subred 192.168.30.0/24 desde el R1 al servidor web. Veamos:

```
R1(config-ext-nacl)#deny icmp 192.168.30.0 0.0.0.255 host 10.10.10.12
R1(config-ext-nacl)#exit
R1(config)#int s0/0/0
R1(config-if)#ip acc
R1(config-if)#ip access-group ACL1 o
R1(config-if)#ip access-group ACL1 out
R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

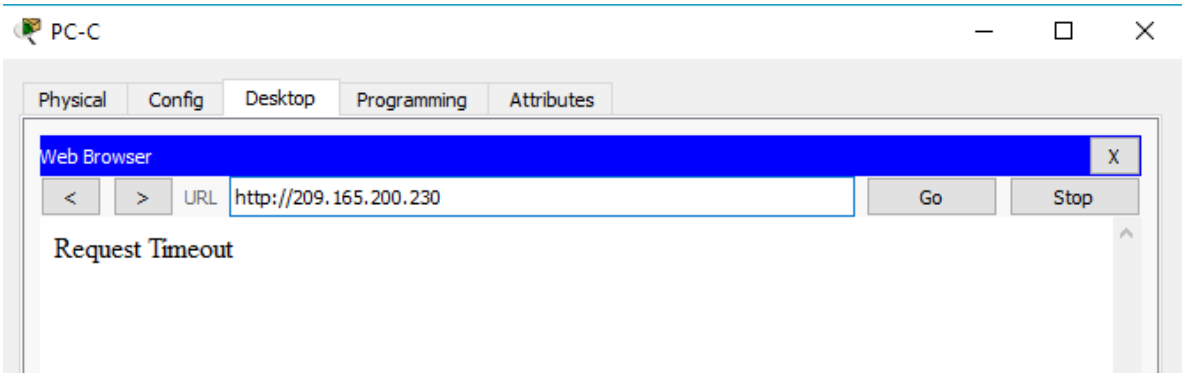
Verificamos haciendo ping desde la PC-A (VLAN 30) hacia el servidor:

```
C:\>ping 10.10.10.12

Pinging 10.10.10.12 with 32 bytes of data:

Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.

Ping statistics for 10.10.10.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

En la segunda lista extendida (ACL2), se va a restringir el acceso a la página web, desde la PC-C (VLAN 40). Veamos:

```
R1(config-ext-nacl)#deny tcp host 192.168.40.31 host 10.10.10.12 eq www established
R1(config-ext-nacl)#exit
R1(config)#int s0/0/0
R1(config-if)#ip acc
R1(config-if)#ip access-group ACL2
% Incomplete command.
R1(config-if)#ip acc
R1(config-if)#ip access-group ACL2 o
R1(config-if)#ip access-group ACL2 out
R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

Ingresamos a la página web desde la PC-C (VLAN 40)



Por último, se verifica las listas de control de acceso extendidas:

```
R1#show access-lists
Extended IP access list ACL1
    10 deny icmp 192.168.30.0 0.0.0.255 host 10.10.10.12 (4 match(es))
Extended IP access list ACL2
    10 deny tcp host 192.168.40.31 host 10.10.10.12 eq www established (1 match(es))
```

NOTA: Si se elimina las listas de acceso extendidas configuradas en el R1, el tráfico de las VLAN hacia las otras sedes fluirá sin ningún problema.

11. VERIFICAR PROCESOS DE COMUNICACIÓN Y REDIRECCIONAMIENTO DE TRÁFICO EN LOS ROUTERS MEDIANTE EL USO DE PING Y TRACEROUTE

Pings desde el R1

```
R1#ping 10.10.10.12

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.12, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/13 ms

R1#ping 192.168.7.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.7.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/12/40 ms

R1#ping 172.31.23.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.23.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/8/21 ms
```

Tracerouter desde R1

```
R1#traceroute 10.10.10.12
Type escape sequence to abort.
Tracing the route to 10.10.10.12

  1   172.31.21.1     37 msec   1 msec    1 msec
  2   10.10.10.12     1 msec    10 msec   5 msec
R1#tracer
R1#traceroute 192.168.7.10
Type escape sequence to abort.
Tracing the route to 192.168.7.10

  1   172.31.21.1     17 msec   1 msec    0 msec
  2   192.168.7.10    1 msec    11 msec   0 msec
R1#tracer
R1#traceroute 192.168.4.10
Type escape sequence to abort.
Tracing the route to 192.168.4.10

  1   172.31.21.1     1 msec    1 msec    0 msec
  2   172.31.23.2     0 msec    10 msec   5 msec
  3   192.168.4.10    16 msec   1 msec    1 msec
```

Pings desde R2

```
R2#ping 192.168.4.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/10 ms

R2#ping 192.168.5.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/7/20 ms

R2#ping 172.31.21.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.21.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/11/27 ms
```

Traceroute desde R2

```
R2#traceroute 192.168.4.10
Type escape sequence to abort.
Tracing the route to 192.168.4.10

  1   172.31.23.2     0 msec    0 msec    1 msec
  2   192.168.4.10    12 msec   0 msec    1 msec
R2#tra
R2#traceroute 192.168.5.10
Type escape sequence to abort.
Tracing the route to 192.168.5.10

  1   172.31.23.2     20 msec   1 msec    1 msec
  2   192.168.5.10    0 msec    1 msec    11 msec
R2#tra
R2#traceroute 172.31.21.2
Type escape sequence to abort.
Tracing the route to 172.31.21.2

  1   172.31.21.2     13 msec   1 msec    6 msec
```

Pings desde R3

```
R3#ping 172.31.21.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.21.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/9/34 ms

R3#ping 10.10.10.12

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.12, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/9/34 ms

R3#ping 192.168.7.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.7.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/8/26 ms
```

Traceroute desde R3

```
R3#traceroute 172.31.21.2
Type escape sequence to abort.
Tracing the route to 172.31.21.2

  1   172.31.23.1     1 msec    0 msec    1 msec
  2   172.31.21.2     8 msec    1 msec    1 msec
R3#traceroute 10.10.10.12
Type escape sequence to abort.
Tracing the route to 10.10.10.12

  1   172.31.23.1     17 msec   2 msec    0 msec
  2   209.165.200.230 0 msec    10 msec   0 msec
R3#traceroute 192.168.7.10
Type escape sequence to abort.
Tracing the route to 192.168.7.10

  1   172.31.23.1     22 msec   7 msec    0 msec
  2   192.168.7.10    12 msec   1 msec    1 msec
```

BIBLIOGRAFIA

CISCO. (2014). Introducción a redes conmutadas. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module1/index.html#1.0.1.1

CISCO. (2014). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1

CISCO. (2014). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1

CISCO. (2014). Enrutamiento Estático. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1

CISCO. (2014). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1

CISCO. (2014). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1

CISCO. (2014). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1

CISCO. (2014). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1

CISCO. (2014). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1