**Configuración S1**

**-----------------------------**

vlan 20

name Contabilidad

vlan 10

name Ingenieria

vlan 99

name Administrativa

int fa0/6

**Configuración S2**

**-----------------------------**

vlan 20

name Contabilidad

vlan 10

name Ingenieria

vlan 99

name Administrativa

! El nombre no importa, el número de vlan si debe corresponder

! entre todos los switches que están conectados.

int vlan 99

ip address 192.168.99.3 255.255.255.0

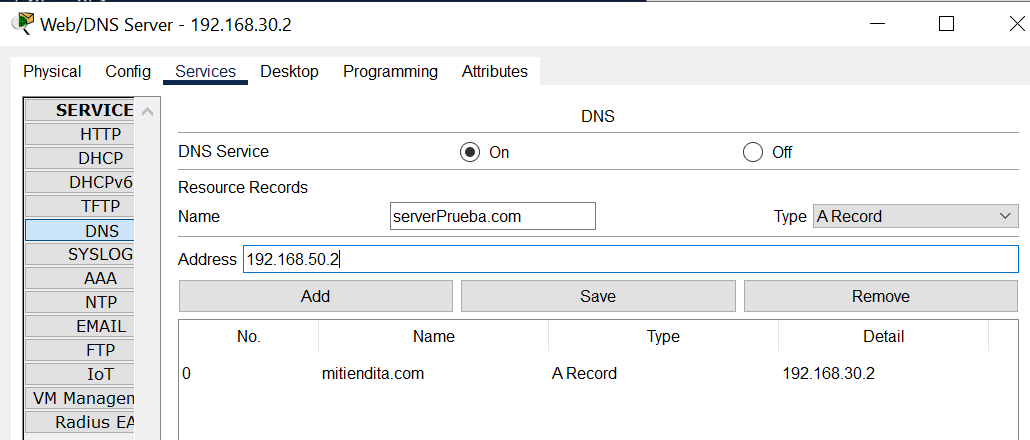
int fa0/6

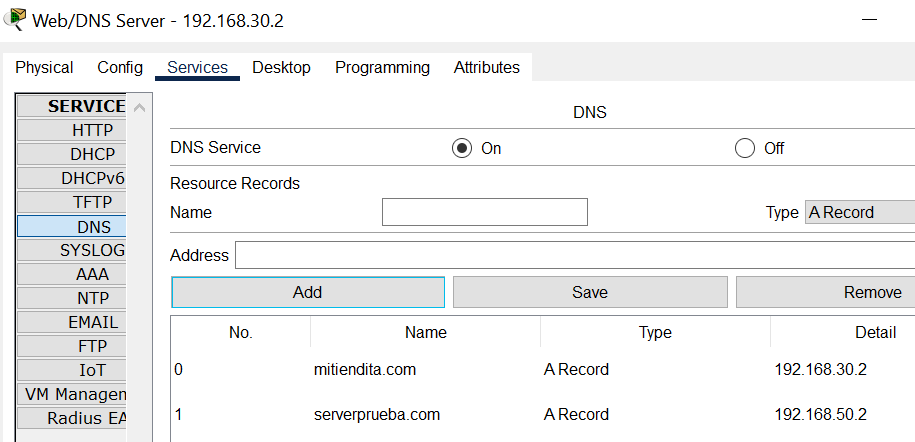




Cada interfaz me cuesta 6000 pesos.

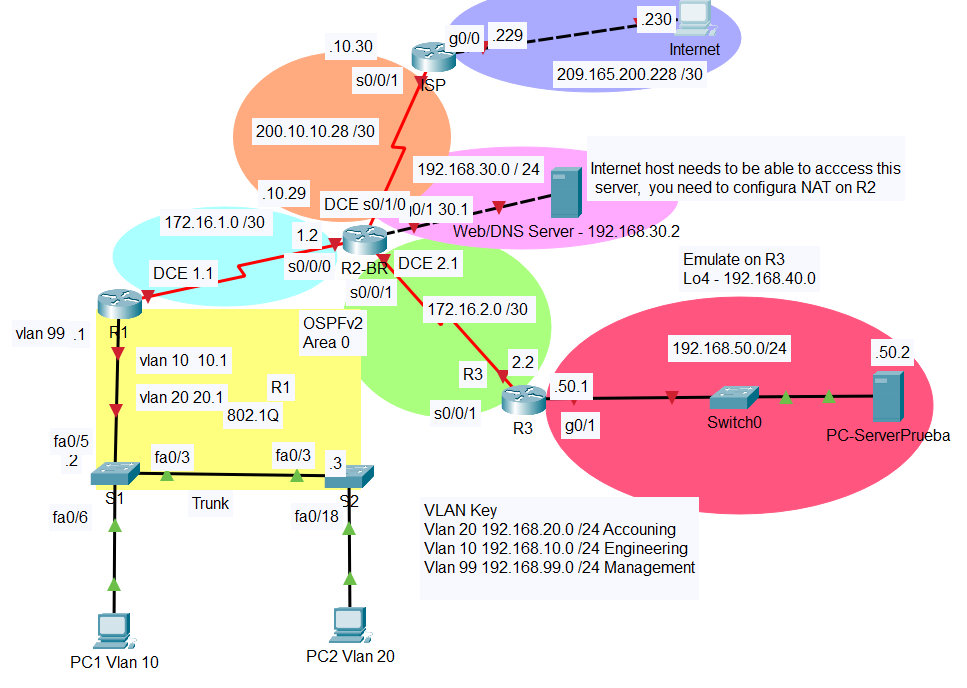
Agregamos al servidor de prueba al servicio de DNS.



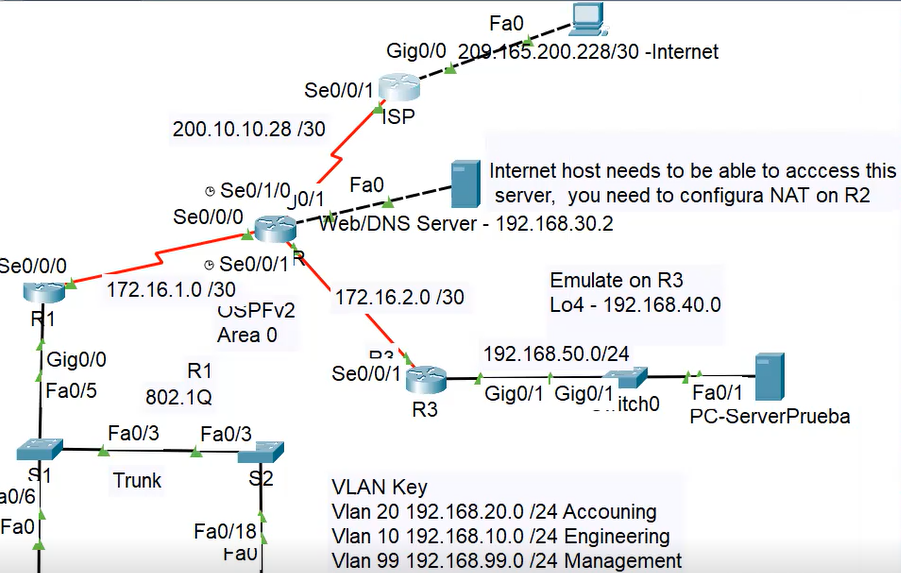


Y ya voy a tener dos nombres que resuelve mi DNS.

Pruebo haciendo ping del servidor al DNS y si jala está bien.



Hasta este punto todos podemos hacer ping con los equipos de al lado o con los equipos vecinos.



Regla que solemos utilizar, la primera IP de la subred se asigna al router.

**ROUTER R2 CONFIGURACIÓN OSPF**

router ospf 1

network 172.16.2.0 0.0.0.3 area 0

!\*

network 192.168.30.0 0.0.0.255 area 0

network 172.16.1.0 0.0.0.3 area 0

passive-interface g0/1

passive-interface s0/1/0

!\*

! En cada red espero se levante la adjacencia con su red vecina

! Ya se levantó la adjacencia, ya hay dos routers hablando OSPF

! Solo agrego las redes que están dentro de mi corporación

!----------------

! El área 0, es simplemente porque con el protocolo OSPF

! tú puedes configurar múltiples áreas, cuando tienes

! una red super grande como la del tec

! de monterrey real, puedes agrupar regiones y cada región

! es un área y el área 0 interconecta a todas las áreas.

! La ventaja de fraccionar en áreas es que si una red se

! cae, solamente se propaga eso dentro de su área y no afecta

! a todo el sistema autónomo de la organización.

! Por eso solamente se fracciona en áreas.

! Cuando la red no es tan grande, como en este caso que

! solamente tenemos tres routers de la organización,

! normalmente todos los routers se ponen en el área 0.

! La red que va al proveedor no se mete, porque esa red

! no es mia (200.10.10.28). Solo agrego las redes que forman

! parte de la organización dentro de las cuales se van a

! desplegar las actualizaciones del ruteo.

! Esta red es del proveedor de servicios y el me cobra por

! conectarme a esa red (200.10.10.28) y a ese enlace

! (209.165.200.228) que me manda hacia

! Internet.

! Este router es el router frontera o border router,

! debemos crear la ruta estática por default y propagarla

! hacia los routers de la organización

default-information originate

ip route 0.0.0.0 0.0.0.0 s0/1/0

----------------------------------------------

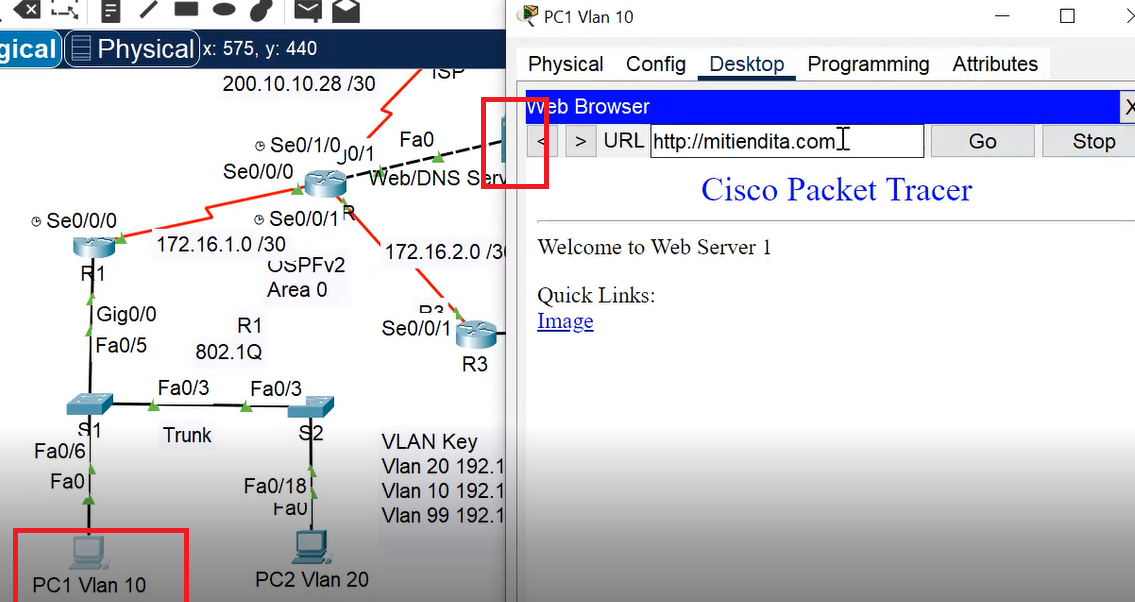


Le doy sh ip route y aquí vemos que ya aprendió la ruta default. Y además ya aprendió redes por OSPF.

Ya podemos hacer ping entre los servidores.

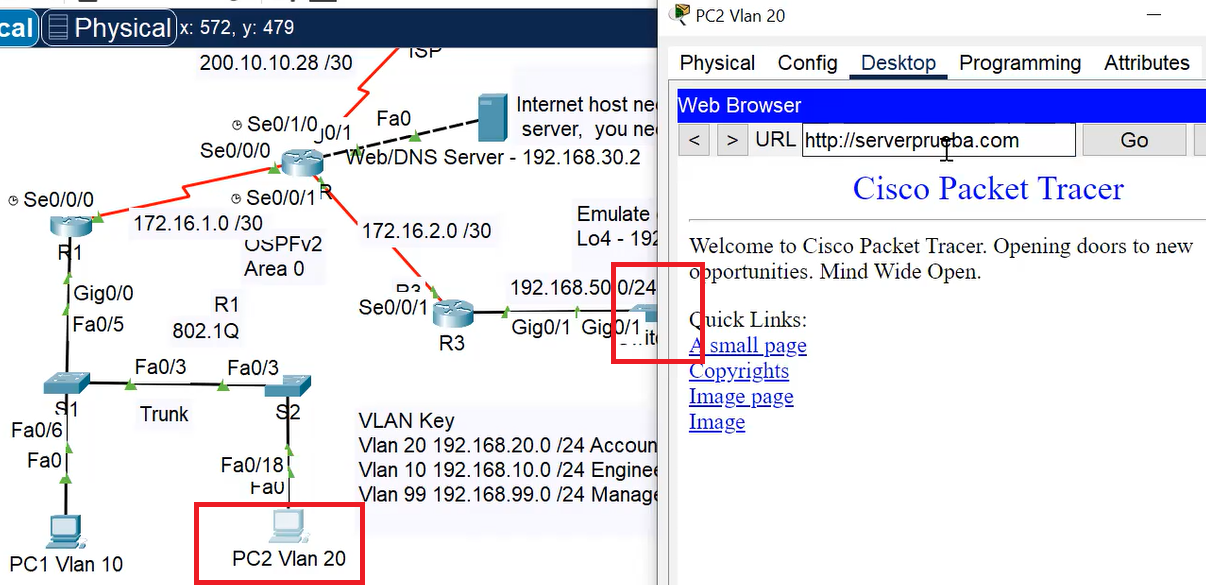
Configuramos OSPF en el router 1

Probamos que desde la PC con web browser haya conectividad a mitiendita.com



Si jala el dns funcionando bien.

Desde la PC2 accedemos al otro servidor de prueba.



Ya tenemos red empresarial funcional, que falta traducir direcciones para que salgan a Internet y poner alguna lista de acceso para representar un firewall.

La organización compró esta red: **200.10.10.0/27**.

La compañía compró la subred 200.10.10.0 /27 debe usrse para NAT.

8.) Traduzca las PCs de la VLAN de Ingeniería usando NAT usando las primeras 15 direcciones compradas.

Las primeras quince IPs compradas son: 200.10.10.1 - .15

Permitir a los host de Internet (simulados por la red 209.165.200.228) el acceso por web al servidor 1 en R2 a través de la dirección estática NAT 200.10.10.20.

Traducir la ip privada del servidor web **192.168.30.2** por la dirección **200.10.10.20**.

**ip nat inside source** { **list** {**Número | Nombre**} **pool** **NOMBRE [overload] | static IP-local IP-Global** }

8.) Traduzca las PCs de la VLAN de Ingeniería usando NAT usando las primeras 15 direcciones compradas. Y como es de la 1 a la 15 de la dirección

200.10.10.0 /27 es la mitad de esa subred, por lo que se va a convertir de /27 a /28.

Traducción NAT y traducción con estático.

Primero realizaremos la traducción estática de la IP privada del servidor web por la dirección pública asignada 200.10.10.20.

**ip nat inside source** **static 192.168.30.2 200.10.10.20**

! Configurar interfaces inside y outside

int g0/1

ip nat inside

! Por aquí van a entrar las direcciones que serán traducidas.

int s0/1/0

ip nat outside

!Por donde van a salir las direcciones que ya han sido traducidas.

En el ISP aún no se coloca la ruta por default, no se puede

probar todavía.

8.) Traduzca las PCs de la VLAN de Ingeniería usando NAT usando las primeras 15 direcciones compradas. Y como es de la 1 a la 15 de la dirección

200.10.10.0 /27 es la mitad de esa subred, por lo que se va a convertir de /27 a /28.

Hay que definir el tráfico a traducir a través de una lista de acceso. Primero hay que definir las direcciones que serán traducidas.

**Ruta estática ISP**

! Ahora hay que sumarizar la red 200.10.10.28 con las direcciones

! públicas de NAT asignadas para la traducción

! 200.10.10.1 - .15 /28 (200.10.10.0/28) y la ip del servidor 200.10.10.20

! Como podemos sumarizar, que equipos tendrían salida hacia Internet

! El web server y la red de ingeniería podría salir hacia Internet.

! Esta ruta la agregaría en el ISP para que devuelva el tráfico desde Internet

! hacia r1 y hacia el servidor web

ip route 200.10.10.0 255.255.255.224 s0/0/1

Sumarizamos las direcciones públicas, la dirección del servidor y la

dirección directamente conectada.

200.10.10.000 1 1100 255.255.255.252 200.10.10.28

200.10.10.000 1 0100 255.255.255.224 200.10.10.20 Servidor

200.10.10.000 0 0000 255.255.255.224 200.10.10.0 Direcciones públicas

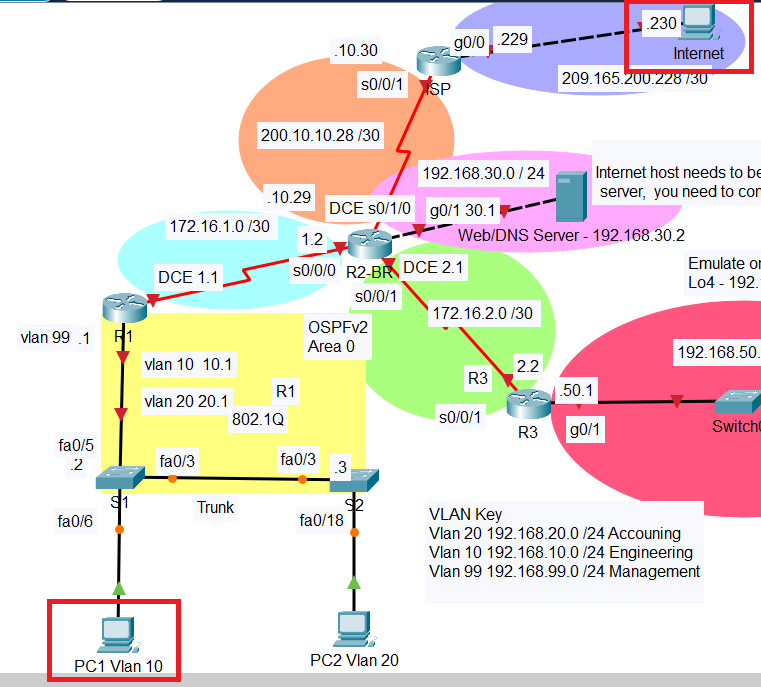
------------------------------------

200.10.10.000 0 0000 255.255.255.224 red sumarizada.

Ya sumaricé, ya puedo salir a Internet, quien va a poder salir a internet:

Los de la vlan de ingeniería

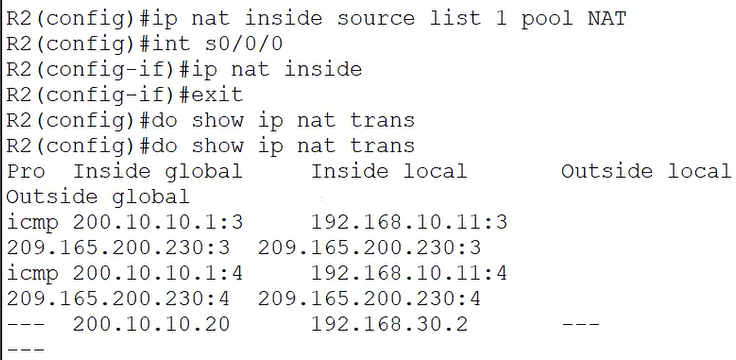
Hago ping de la pc1 hacía Internet si jala.



En el router 2 ejecutamos el comando

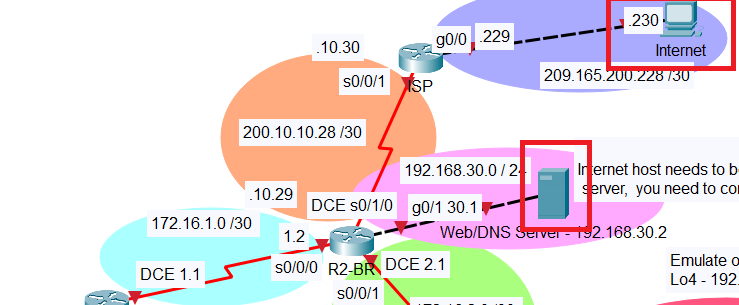
sh ip nat trans

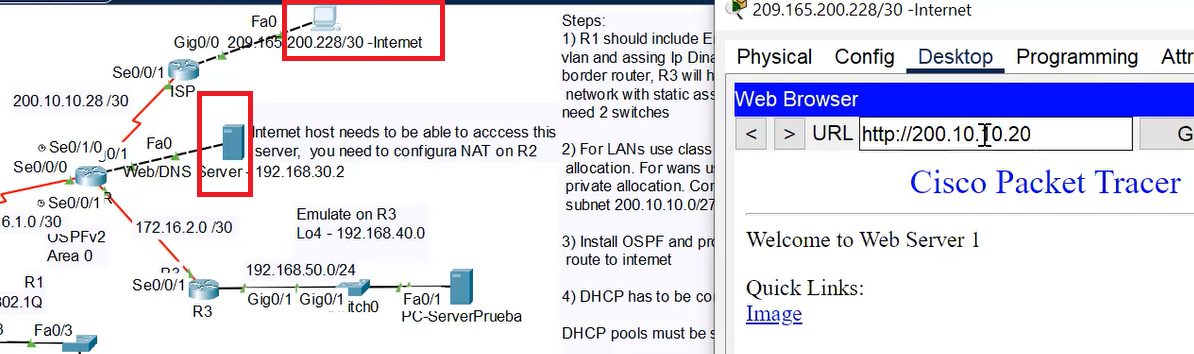
Podemos observar que la ip 192.168.10.11 se está traduciendo con una dirección ip pública 200.10.10.1



La red original que se compró tiene 32 host 200.10.10.0 /27

Desde el Intenet debemos acceder al servidor público de la organización, el web server.

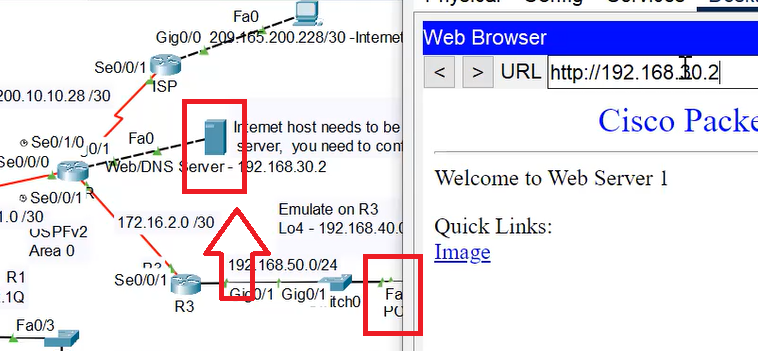




Si funciona. Se sugiere probar de nuevo sh ip nat trans

Si el servidor web lo quiero acceder desde fuera de la organización debo usar la ip pública (200.10.10.20), si lo quiero acceder dentro de la organización el servidor lo debo acceder con la dirección privada (192.168.30.2), ya que dentro de la organización no se conocen las redes públicas.

Por ejemplo, acceder por web desde el servidor de prueba al servidor de web 192.168.30.2 funciona.



**ACLS**

Nos falta configurar un pequeño cortafuegos:

Prevent traffic from the Internet from pinging internal networks, while continuing to allow LAN interfaces to ping the Internet PC

+Permit the access only to web services(web server) the rest of the internet traffic should be block

Apply ACL to the appropriate interfaces.

Verify ACL is working as expected

**Evite que el tráfico de Internet haga ping en las redes internas, mientras continúa permitiendo que las interfaces LAN hagan ping en la PC con Internet**

**+Permitir el acceso solo a los servicios web (servidor web), el resto del tráfico de Internet debe bloquearse**

**Aplique ACL a las interfaces apropiadas.**

**+Permitir el acceso solo a los servicios web (servidor web), el resto del tráfico de Internet debe bloquearse**

Cuando hablamos de cortafuegos

1. La primera barrera de protección en mi red es bloquea todo y solo abre los puertos de tus servidores públicos

Vamos a configurar el firewall en el ruteador 2

ip access-list extended FIREWALL

permit tcp any host 200.10.10.20 eq 80

permit tcp any host 200.10.10.20 eq 443

configuramos la ip pública del servidor.

**Evite que el tráfico de Internet haga ping en las redes internas, mientras continúa permitiendo que las interfaces LAN hagan ping en la PC con Internet**

**En pocas palabras que no me puedan hacer ping de afuera de mi red, pero que mis ingenieros PCs puedan pinguear hacia afuera.**

**permit icmp any any echo-reply**

Para permitir solamente la entrada de las respuestas de los pings.

A ping is a transaction. You send and echo request, you get an echo reply, Ping uses the ICMP protocol.  The source will send an ICMP echo request to the destination device, and wait for the destination to respond back with a echo reply. If the source does not receive an echo reply, there is a connectivity issue then.But then a ping faliure does not always mean a connection problem, it could also mean that the network device is reachable, but the source isn't authorized to access it.

How

     1. Source generates a ICMP messge, which is encapsulated in the IP datagram. **This is the Echo request to be sent out.**

     2. This IP datagram has the source and destination IP address

1. The destination receives it, sees the destination address **and sends a echo reply back to the originating device**.

! FALTA aplicar la lista de acceso a la interfaz para que filtre

! trafico y bloque tráfico por consiguiente.

! En qué interfaz lo vamos a aplicar y en qué sentido.

! Queremos filtrar el tráfico de Internet hacia el interior de la red.

! Cuál es la intefaz que nos conecta hacia Internet la interfaz s0/1/0.

! Ahí vamos a colocar nuestro cortafuegos y en qué sentido?

! En qué sentido quiero filtrar, quiero filtra el tráfico que proviene

! o entra de Internet.

**int s0/1/0**

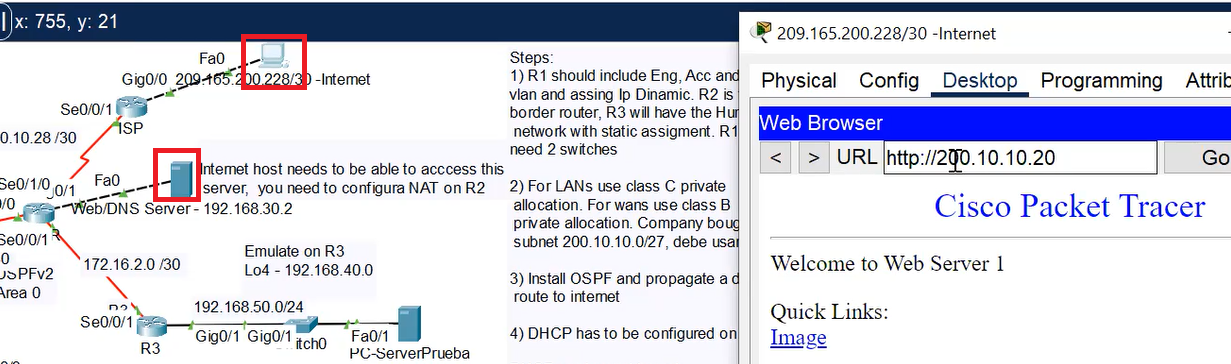
**ip access-group FIREWALL in**

! in (tráfico de entrada)

Ya no puedo hacer ping del internet hacia el servidor, la dirección pública.

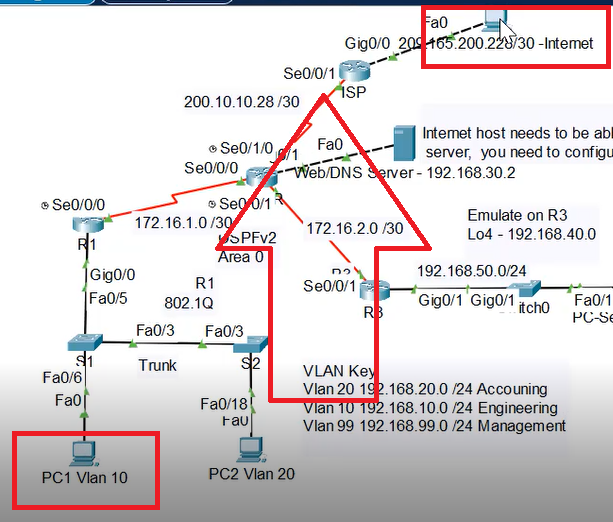


Sin embargo si abro el navegador, como el navegador es lo único que estamos permitiendo con el cortafuegos, entonces el navegador si debe funcionar.



Si funciona el acceso por web.

Por último para probar que los pings siguen regresando, vamos a hacer un ping desde la única vlan que puedo salir hacia el exterior y me sigue permitiendo que llegue de regreso.



Pero si yo quiero hacer ping del Internet hacia el interior no voy a poder, ya que el echo request está bloqueado.