

Practica Redes

20-intro-a-redes:

1- Setear IP y mascara sub red, para comunicarse tienen que pertenecer a la misma red, ósea misma sub mascara. Ver la dirección de la red

2- Se puede hacer ping con el sobre o mediante la aplicación command prompt y el comando ping. Ej: ping 192.168.2.1
Primero se genera el ping, después se envía y en 3er lugar vuelve la respuesta, sí lo vemos en el panel de simulación

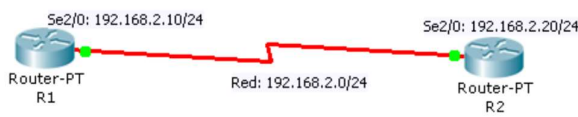
3- Hub lo que llega por un puerto lo retransmite a todo los demás. Si coloco un switch hay que **esperar que se pongan en verde las luces antes de simular**.

El switch reenvía el mensaje en función de la dirección MAC. El arma una tabla donde tiene asociado cada puerto con la MAC conectada. Y envía el mensaje solo a quien corresponde, no a todos.

21-capa-de-enlace PPP: Ejemplo de conexión entre router PPP

En el siguiente esquema de red (**ppp_chap.pkz**)

Lo verde solo se puede hacer por consola.



Router 1

```
R1>enable
R1#configure terminal
R1(config)#hostname R1
R1(config)#username R2 password aaaa
R1(config)#interface serial2/0
R1(config-if)#ip address 192.168.2.10
255.255.255.0
R1(config-if)#clock rate 128000
R1(config-if)#encapsulation ppp
R1(config-if)#ppp authentication chap
R1(config-if)#no shut
R1(config-if)#end
```

Router 2

```
R2>enable
R2#configure terminal
R2(config)#hostname R2
R2(config)#username R1 password aaaa
R2(config)#interface serial2/0
R2(config-if)#ip address 192.168.2.20
255.255.255.0
R2(config-if)#encapsulation ppp
R2(config-if)#ppp authentication chap
R2(config-if)#no shut
R2(config-if)#end
```

Configuración de Routers

Router 1

R1>enable

R1#configure terminal

R1(config)#hostname R1 *Configuro el nombre del router*

R1(config)#username R2 password aaaa *Le indico el password para comunicarse con el usuario R2*

R1(config)#interface serial2/0 *Para acceder a la configuración de la interfase o puerto*

R1(config-if)#ip address 192.168.2.10 255.255.255.0

R1(config-if)#clock rate 128000

R1(config-if)#encapsulation ppp

R1(config-if)#ppp authentication chap

R1(config-if)#no shut *Encender el Puerto*

R1(config-if)#end

Hacer un ping desde el Router R1 al router R2. Desde la consola de R1 hacemos:

R1>enable

R1#ping 192.168.2.10

Para ver la configuración del puerto serial 2/0.

R1>enable

R1#show interface serial2/0

Observe el tipo de encapsulación que utiliza, guarde esta configuración.

En el siguiente esquema de red (**ppp_pap.pkz**)

Router 1

```
R1>enable
R1#configure terminal
R1(config)#hostname R1
R1(config)#username R2 password aaaa
R1(config)#interface serial2/0
R1(config-if)#ip address 192.168.2.10
255.255.255.0
R1(config-if)#clock rate 128000
R1(config-if)#encapsulation ppp
R1(config-if)#ppp authentication pap
R1(config-if)#ppp pap sent-username R1
password aaaa
R1(config-if)#no shut
R1(config-if)#end
```

Router 2

```
R2>enable
R2#configure terminal
R2(config)#hostname R2
R2(config)#username R1 password aaaa
R2(config)#interface serial2/0
R2(config-if)#ip address 192.168.2.20
255.255.255.0
R2(config-if)#encapsulation ppp
R2(config-if)#ppp authentication pap
R2(config-if)#ppp pap sent-username R2
password aaaa
R2(config-if)#no shut
R2(config-if)#end
```

Router 1

```
R1>enable
R1#configure terminal
R1(config)#hostname R1
R1(config)#username R2 password aaaa
R1(config)#interface serial2/0
R1(config-if)#ip address 192.168.2.10 255.255.255.0
R1(config-if)#clock rate 128000
R1(config-if)#encapsulation ppp
R1(config-if)#ppp authentication pap
R1(config-if)#ppp pap sent-username R1 password aaaa
R1(config-if)#no shut
R1(config-if)#end
```

Para ver la configuración del puerto serial 2/0.

```
R1>enable
R1#show interface serial2/0
```

Observe el tipo de encapsulación que utiliza, guarde esta configuración.

Para ver la negociación del protocolo PPP utilizamos los comandos:

```
R1#debug ppp authentication
R1#debug ppp negotiation
```

Luego podemos apagar en puerto del modem y volver a encender, así vemos la comunicación entre modem.

22- capa-de-enlace Ethernet

El IEEE ha estandarizado varias redes de área local y de área metropolitana bajo el nombre de IEEE 802.

- 802.3 (Ethernet)
- 802.11 (LAN inalámbrica).
- 802.15 (Bluetooth)
- 802.16 (MAN inalámbrica).

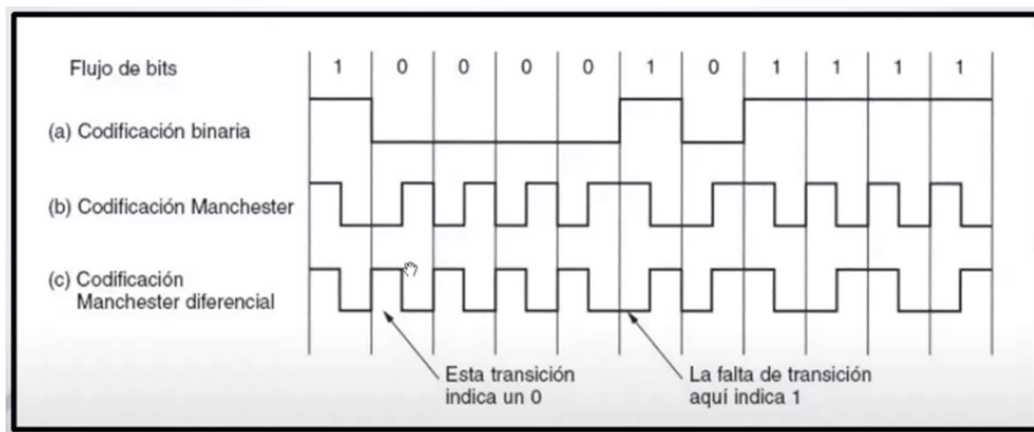
802.3 y 802.11 tienen diferentes capas físicas y diferentes subcapas MAC, pero convergen en la misma subcapa de control lógico del enlace LLC (802.2), por lo que tienen la misma interfaz a la capa de red.

Codificación Manchester y codificación Manchester diferencial

Ethernet no utiliza codificación binaria directa, las diferencias de velocidades de reloj pueden causar que el receptor y el emisor pierdan la sincronía.

En la codificación Manchester, cada periodo de bit se divide en dos intervalos iguales. Un bit 1 binario se envía teniendo el voltaje alto durante el primer intervalo y bajo durante el segundo. Un 0 binario es justo lo inverso: primero bajo y después alto.

La codificación Manchester diferencial, un bit 1 se indica mediante la ausencia de una transición al inicio del intervalo. Un bit 0 se indica mediante la presencia de una transición al inicio del intervalo. En ambos casos también hay una transición a la mitad.



Una desventaja de la codificación Manchester y Manchester diferencial es que requiere el doble de ancho de banda que la codificación binaria directa, pues los pulsos son de la mitad de ancho.

48 bits

Trama Ethernet

8 bytes	6 bytes	6 bytes	2 bytes	0-1500 b	0-46 b	4 bytes
Preámbulo	Dirección destino	Dirección Origen	Tipo	Datos	Relleno	Suma de verificación

La trama comienza con un Preámbulo de 7 bytes, cada uno de los cuales contiene el patrón de bits 10101010, más 1 byte llamado inicio de trama. El preámbulo sirve para que el receptor se sincronice.

Luego del inicio de trama, siguen dos direcciones (MAC), destino y origen. El bit de orden mayor de la dirección de destino es 0 para direcciones ordinarias y 1 para direcciones de grupo. Las direcciones de grupo permiten que todas las estaciones del grupo la reciban. El envío a un grupo de estaciones se llama **multidifusión** (*multicast*). La dirección que consiste en todos los bits en 1 se llama para **difusión** (*broadcast*). Una trama de multidifusión se envía a un grupo seleccionado de estaciones de la Ethernet; una trama de difusión se envía a todas las estaciones de la Ethernet.

Trama 802.3

8 bytes	6 bytes	6 bytes	2 bytes	0-1500 b	0-46 b	4 bytes
Preámbulo	Dirección destino	Dirección Origen	Longitud	Datos	Relleno	Suma de verificación

El campo de *Tipo* (Ethernet DIX), que indica al receptor qué hacer con la trama. Es posible utilizar múltiples protocolos de capa de red al mismo tiempo en la misma máquina, por lo que cuando llega una trama de Ethernet, el *kernel* debe saber a cuál entregarle la trama. El campo longitud (IEEE 802.3), indica la longitud de la trama. En la actualidad los números menores o iguales a 1500 son longitudes y los mayores son tipo.

El emisor calcula el CRC de toda la trama, desde el campo destino

Trama 802.3 y trama Ethernet

Los datos poseen una longitud mínima de 0 y hasta 1500 bytes.

El límite de 1500 bytes fue elegido de manera algo arbitraria cuando se estableció el estándar DIX, con base en el hecho de necesitar suficiente RAM para mantener toda una trama y la RAM era muy costosa.

Las tramas deben tener como mínimo 64 bytes, desde la dirección de destino hasta la suma de verificación. Si no se llega a esta cantidad se utiliza el campo de relleno (0-46 bytes).

Una trama debe tener una longitud mínima para evitar que una estación complete la transmisión de una trama corta antes de que el primer bit llegue al extremo más alejado del cable, donde podría tener una colisión con otra trama.

ARP—Protocolo de Resolución de Direcciones

Aunque cada host tiene una (o más) direcciones IP, éstas no pueden usarse para enviar paquetes porque el hardware de capa de enlace de datos no entiende las direcciones IP. Cada tarjeta Ethernet viene provista de fábrica con una dirección Ethernet de 48 bits (MAC). Los fabricantes de tarjetas Ethernet solicitan un bloque de direcciones a una autoridad central para asegurar que dos tarjetas no tengan la misma dirección. Las tarjetas envían y reciben tramas basadas en direcciones Ethernet de 48 bits. No saben nada de direcciones IP de 32 bits.

IMPORTANTE

ARP: Protocolo de resolución de direcciones, es un protocolo responsable de encontrar la dirección hardware (Ethernet MAC) que corresponde a una determinada dirección IP, es decir resuelve el problema de encontrar qué dirección Ethernet corresponde a una dirección IP dada.

La definición de ARP está en el RFC 826.

ARP es un protocolo de capa 2 y 3 del modelo OSI, se ubica entre ambas capas.

ARP—Protocolo de Resolución de Direcciones

IMPORTANTE

Funcionamiento:

Se envía un paquete (ARP request) a la dirección de difusión de la red (broadcast → MAC = FF FF FF FF FF FF) que contiene la dirección IP por la que se pregunta, y se espera a que esa máquina (u otra) responda (ARP reply) con la dirección Ethernet que le corresponde.

Cada máquina mantiene una tabla con las direcciones traducidas para reducir el retardo y la carga.

ARP permite a la dirección de Internet ser independiente de la dirección Ethernet, pero esto sólo funciona si todas las máquinas lo soportan.

Para permitir que las direcciones físicas cambien, por ejemplo, cuando una tarjeta Ethernet falla y se reemplaza con una nueva (nueva dirección Ethernet), las entradas en la tabla ARP deben expirar en unos cuantos minutos.

RARP -Protocolo de Resolución de Dirección de Retorno

RARP: Este protocolo permite que un host recientemente inicializado transmita su dirección Ethernet y pregunte por su dirección IP.

El servidor RARP ve esta solicitud, busca la dirección Ethernet en sus archivos de configuración y devuelve la dirección IP correspondiente.

RARP está definido en el RFC 903.

RARP es un protocolo de capa 2 y 3 del modelo OSI, se ubica entre ambas capas.

VLAN (LAN Virtual)

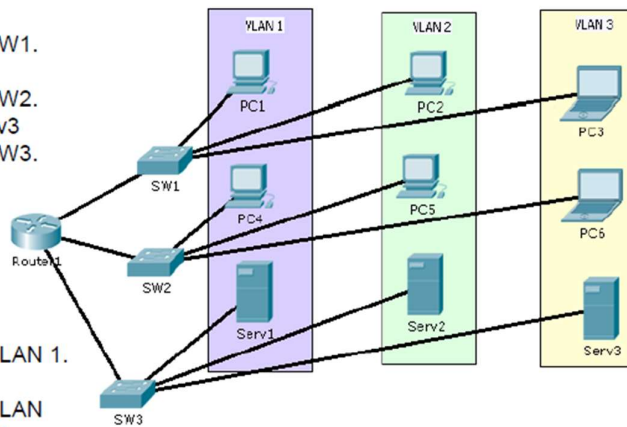
Una VLAN es un método de crear redes lógicas e independientes dentro de una misma red física.

Una VLAN consiste en una red de host que se comportan como si estuviesen conectados al mismo switch, aunque pueden estar en realidad conectados físicamente a diferentes segmentos de una red de área local.

- Varias VLANs pueden coexistir en un único switch físico o en una única red física.
- Ayudan en la administración de la red separando segmentos lógicos de una LAN (como departamentos de una empresa) que no deberían intercambiar datos usando la red local.
- Los administradores de red configuran las VLANs mediante software en lugar de hardware, lo que las hace extremadamente flexibles.
- Una de las mayores ventajas de las VLANs surge cuando se traslada físicamente algún host a otra ubicación: puede permanecer en la misma VLAN sin necesidad de cambiar la configuración IP de la máquina.

VLAN (LAN Virtual)

Los host PC1, PC2 y PC3 conectadas físicamente al SW1.
Los host PC4, PC5 y PC6 conectadas físicamente al SW2.
Los host Serv1, Serv2 y Serv3 conectadas físicamente al SW3.



Los host PC1, PC4 y Serv1 lógicamente conectadas a VLAN 1.
Los host PC2, PC5 y Serv2 lógicamente conectadas a VLAN 2.
Los host PC3, PC6 y Serv3 lógicamente conectadas a VLAN 3.

Siempre seguir el orden de conexión indicado en la pantalla, sino no lo toma.

Los PUERTOS de un Router tienen distintas MAC???

La primer dirección IP de la red, generalmente es el GATEWAY por defecto. Ósea la dirección IP del puerto del Router

Logical [Root] New Cluster Move Object Set Tiled Background Viewport

Red 192.192.192.0/24 Red 177.176.175.0/16

PC1 Hub0 Router0 Hub1 PC2

Router0 Physical Config CLI

FastEthernet0/1

Port Status ☒ On
Bandwidth ☒ Auto
Duplex ☒ Auto
MAC Address 0000.0000.EEEE
IP Address 177.176.175.1
Subnet Mask 255.255.0.0
Tx Ring Limit 10

Equivalent IOS Commands

```
Router(config)#ip address 192.192.192.1 255.255.255.0  
Router(config)#  
Router(config)#exit  
Router(config)#interface FastEthernet0/1  
Router(config-if)#ip address 177.176.175.1 255.255.0.0  
Router(config-if)#
```

PT Activity

Colocar las siguientes direcciones IP:

- IP PC1: 192.192.192.10/24
- IP PC2: 192.192.192.20/24
- IP PC3: 177.176.175.10/16
- IP Router0 FastEthernet0/0: 192.192.192.1/24
- IP Router0 FastEthernet0/1: 177.176.175.1/16

Completion: 53%
Top Check Results Reset Activity 3/7

Por consola podemos poner el comando `pc>arp -a` para visualizar la tabla
`Pc>arp -d` Limpia la tabla ARP

Los mensajes tienen alcance dentro de la RED, los dispositivos completan su tabla con los datos de los demás dispositivos dentro de su red.

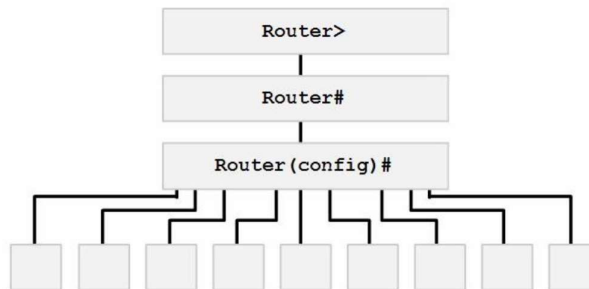
Formas de interpretar la consola:

Modo EXEC de usuario

Modo EXEC privilegiado

Modo de configuración global

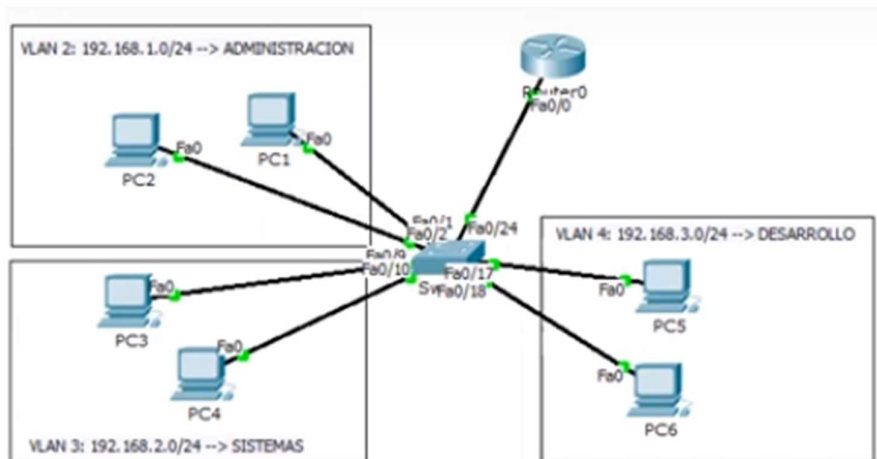
Modo de configuración específico



Modo de configuración	Prompt
Interfaz	Router (config-if) #
Línea	Router (config-line) #
Routers	Router (config-router) #

VLANS:

Las redes VLAN son redes lógicas que nosotros tenemos, y nos van a ayudar a la administración de red, separando segmentos lógicos de Red LAN. Ej: Los departamentos de una empresa.



VLANS

Tenemos 3 redes conectadas a un Switch:

ADMINISTRACION: 192.168.1.0/24
SISTEMAS: 192.168.2.0/24
DESARROLLO: 192.168.3.0/24

/--- VLAN ---/

Crear y configurar en el switch el nombre de VLAN. (no es un Switch común de capa 2, es uno especial de capa 3, que puede trabajar con VLAN)

```
Switch> enable
Switch# configure terminal
Switch(config)# VLAN <Numero de la VLAN>
Switch(config-vlan)# name <Nombre de la VLAN>
Switch(config-vlan)# exit
```

EJ: creamos una nueva VLAN:

```
Switch> enable
Switch1# configure terminal
Switch1(config)#vlan 50
Switch1(config-vlan)#name Alumnos
Switch1(config-vlan)#exit
```

Repetimos todo hasta el exit para cada VLAN nueva.

<u>Asignación de puerto a VLAN para las PCs o usuarios.</u> Switch> enable Switch# config terminal Switch(config)# interface <Nombre de la interfaz> Switch(config-if)# switchport access VLAN <Numero de la VLAN> Switch(config-if)# exit (IMPORTANTE)	<u>Asignemos puertos a esa VLAN</u> Switch1> enable Switch1# configure terminal Switch1(config)# interface fastEthernet0/6 Switch1(config-if)# switchport access VLAN 50 Switch(config-if)# exit Switch1(config)# interface fastEthernet0/11 Switch1(config-if)# switchport access VLAN 50 Switch(config-if)# exit o Switch1(config-if)# end
<u>Asignación de Puerto en el Switch (donde está conectado el router) en modo trunk</u> Switch> enable Switch# config terminal Switch(config)# interface <Nombre de la interfaz donde está conectado el router> Switch(config-if)# switchport mode trunk Switch(config-if)# exit	<u>Configuración de enlaces troncales entre el Switch con el ROUTER</u> Switch1> enable Switch1# configure terminal Switch1(config)# interface gigabitEthernet 0/1 Switch1(config-if)# switchport mode trunk Switch1(config-if)# exit
Configuración del Router (Como si existieran n router, uno para cada VLAN). Dividimos el puerto, una parte para cada VLAN Router> enable Router# config terminal Router(config)# interface <Nombre de la interfaz y la sub dividido en n redes> Router(config-subif)# encapsulation dot1Q 2 (a veces no va esto) Router(config-subif)# ip address <Direccion IP (Gateway)> <Netmask> es para cada sub división lógica de la red. Router(config-subif)# exit	Router> enable Router# config terminal Router(config)# interface gigabitEthernet 0/0.1 Router(config-subif)# encapsulation dot1Q 2 Router(config-subif)# ip address 192.168.1.1 255.255.255.0 Router(config-subif)# exit Router> enable Router# config terminal Router(config)# interface gigabitEthernet 0/0.2 Router(config-subif)# encapsulation dot1Q 3 Router(config-subif)# ip address 192.168.2.1 255.255.255.0 Router(config-subif)# exit

Cuando hago un ping entre maquinas de VLANs distintas, el mensaje va del switch hacia al router como si saliera de la red y este lo devuelve enviándolo a la VLAN que corresponde.

Comandos Útiles

Switch> enable

Switch1#show interfaces trunk

Switch1#show running-config

Switch1#show vlan brief

Switch1# show ip interface brief Estado de los puertos

IGNORAR

Esto lo saque de otra materia por si me servía.

STP

comando **show spanning-tree** Verificamos estado de los puertos

Verificación

Switch# **configure terminal** [enter]

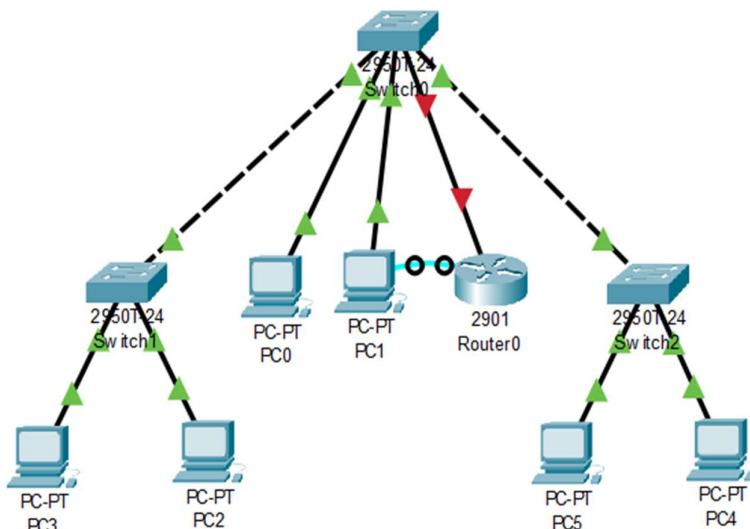
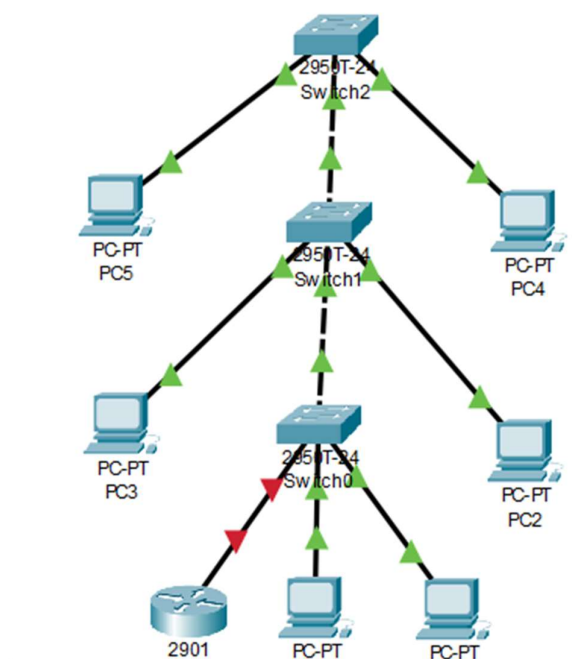
Switch(config)#

Switch(config)# **interface gigabitEthernet 0/1** [enter]

switch(config-if)# **shutdown**

Esperemos un minuto para que se realicen los cambios en STP, y repitamos los comandos *show spanning-tree* en cada switch
Habilitemos nuevamente la interface bloqueada en el paso anterior

```
switch(config-if)# no shutdown [enter]
```



IP	131	.	108	.	122	.	204	IP = 131.108.122.204 / 24 RED = 131.108.122.0 Host1 = 131.108.122.1 Hostn = 131.108.122.254 Broadcast=131.108.122.255
Máscara	255	.	255	.	255	.	0	
RED							Host	

IP	10000011	01101100	01111010	11001100	IP = 131.108.122.204 / 20 RED = 131.108.112.0 Host1 = 131.108.112.1 Hostn = 131.108.127.254 Broadcast = 131.108.127.255
Máscara	255	255	240	0	
Máscara	11111111	11111111	11110000	00000000	
	RED			Host	

Toda la parte de host en 1 para difusión.

$2^n - 2$ = cantidad host, donde n es la cantidad de ceros de la mascara de sub red. Se restan 2 por la dirección de broadcast y la que corresponde al nombre de la red.

Ruteo estático

Previo configurar interfaz, dirección ip, gateway y netmask de cada red.

El enrutamiento estático, es creado manualmente. Para crear una ruta estática el comando a utilizar es el siguiente:

```
router(config)#ip route direccion-red mascara-subred { direccion-ip | interfaz-salida }
```

Con la IP del siguiente salto:

```
ip route [ip red destino][mascara de subred][ip siguiente salto]
```

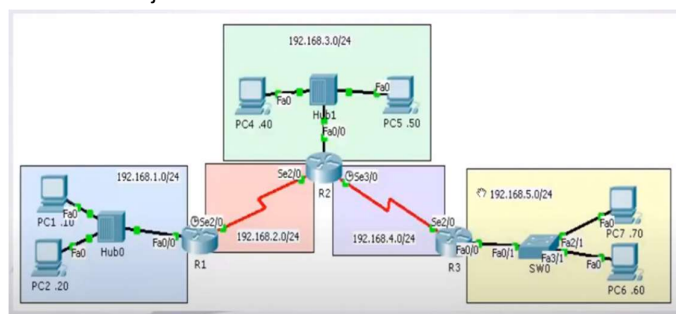
```
ejemplo: R1(config)#ip route 192.168.3.0 255.255.255.0 192.168.2.2
```

Observar que estamos en el R1 y queremos acceder a la red 192.168.3.0/24

Con la interfaz de salida:

```
ip route [ip red destino][mascara de subred][interfaz de salida]
```

ejemplo: R2(config)#**ip route 192.168.3.0 255.255.255.0 serial2/0**



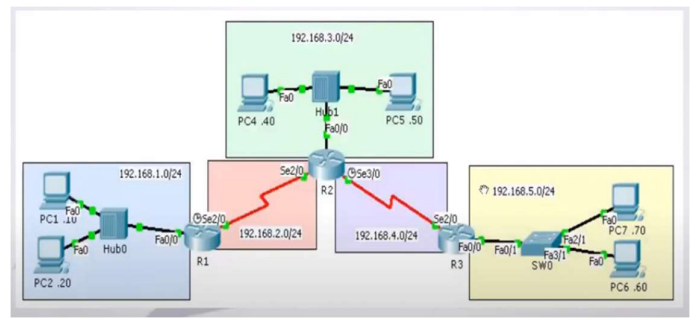
Interfaz de salida, se refiere a la interfaz del router local, que está conectado a las redes externas

Para borrar rutas utilizamos el comando:

```
router(config)#no ip route direccion-red mascara-subred {  
direccion-ip | interfaz-salida }
```

no ip route [ip red destino][mascara de subred][ip siguiente salto]
ejemplo: R1(config)#**no ip route 192.168.3.0 255.255.255.0 192.168.2.2**

no ip route [ip red destino][mascara de subred][interfaz de salida]
ejemplo: R2(config)#**no ip route 192.168.3.0 255.255.255.0 serial2/0**



La dirección IP se mantiene todo el recorrido, pero la MAC va cambiando en cada salto de red.

Ruteo estático por defecto

Con la IP del siguiente salto:

La ruta por defecto le dirá al router que envíe a la dirección ip del siguiente salto, todos los paquetes que tengan como destino una red que no esté incluida en la tabla de enrutamiento.

```
ip route 0.0.0.0 0.0.0.0 [ip interfaz siguiente salto]  
Ejemplo: R1(config)#ip route 0.0.0.0 0.0.0.0 192.168.2.2
```

Con la interfaz de salida:

La ruta por defecto le dirá al router que envíe a la interfaz de salida, todos los paquetes que tengan como destino una red que no esté incluida en la tabla de enrutamiento.

```
ip route 0.0.0.0 0.0.0.0 [interfaz de salida]  
Ejemplo: R1(config)#ip route 0.0.0.0 0.0.0.0 serial2/0
```

NAT y DHCP:

La técnica de NAT, network address translation, que es un cambio de dirección de red. Lo que hace el router intermedio es, todos los paquetes que vengan de la red local y se envíen hacia internet les cambia la dirección origen, cosa que en el destino puedan utilizar la nueva dirección origen para enviar una respuesta.

Esta nueva dirección origen, es la IP pública que tiene el router.

En la ida, tanto en la LAN como en internet la IP destino es la misma, pero la origen varía.

En la vuelta, la IP origen no se modifica, pero la destino sí.

Para esta traducción en el router existen tablas de NAT.

NAT estático

Configuración del Router:

1) Asociar la dirección IP privada a la pública, comando a utilizar:
Router(config)#ip nat inside source static [IP LOCAL] [IP EXTERNA]

2) Indica qué interfaz es la que está conectada a la red interna. Hay que ingresar dentro de la interfaz y e indicarle que es interna
Router(config)#interface [INTERFAZ]
Router(config-if)#ip nat inside
Router(config-if)#exit

3) Indica qué interfaz es la que está conectada a la red externa. Hay que ingresar dentro de la interfaz y e indicarle que es externa
Router(config)#interface [INTERFAZ]
Router(config-if)#ip nat outside
Router(config-if)#exit

NAT dinámico

Configuración del Router:

1) Definimos la **lista de direcciones IP externas** que va a tener el router para asignarle a los paquetes salientes:

```
Router(config)#ip nat pool [NOMBRE DE LISTA DE IPS] [PRIMERA IP]
[ULTIMA IP] netmask [MASCARA DE RED] Calcular las ip publicas con cuidado
```

2) Configurar la lista de acceso para que sepa el rango de direcciones a las que le tiene que aplicar NAT:

```
Router(config)#access-list [NUMERO DE LISTA DE ACCESO] permit [IP
DE RED] [WILDCARD]
```

3) Decirle a NAT con qué lista de acceso va a controlar las IPs que tiene que convertir:

```
Router(config)#ip nat inside source list [NUMERO DE LISTA DE
ACCESO] pool [NOMBRE DE LISTA DE IPS] overload
```

4) Indica qué interfaz es la que está conectada a la red interna. Hay que ingresar dentro de la interfaz y e indicarle que es interna

```
Router(config)#interface [INTERFAZ]
Router(config-if)#ip nat inside
Router(config-if)#exit
```

5) Indica qué interfaz es la que está conectada a la red externa. Hay que ingresar dentro de la interfaz y e indicarle que es externa

```
Router(config)#interface [INTERFAZ]
Router(config-if)#ip nat outside
Router(config-if)#exit
```

Ejemplos:

Configurar NAT estático en SERVER

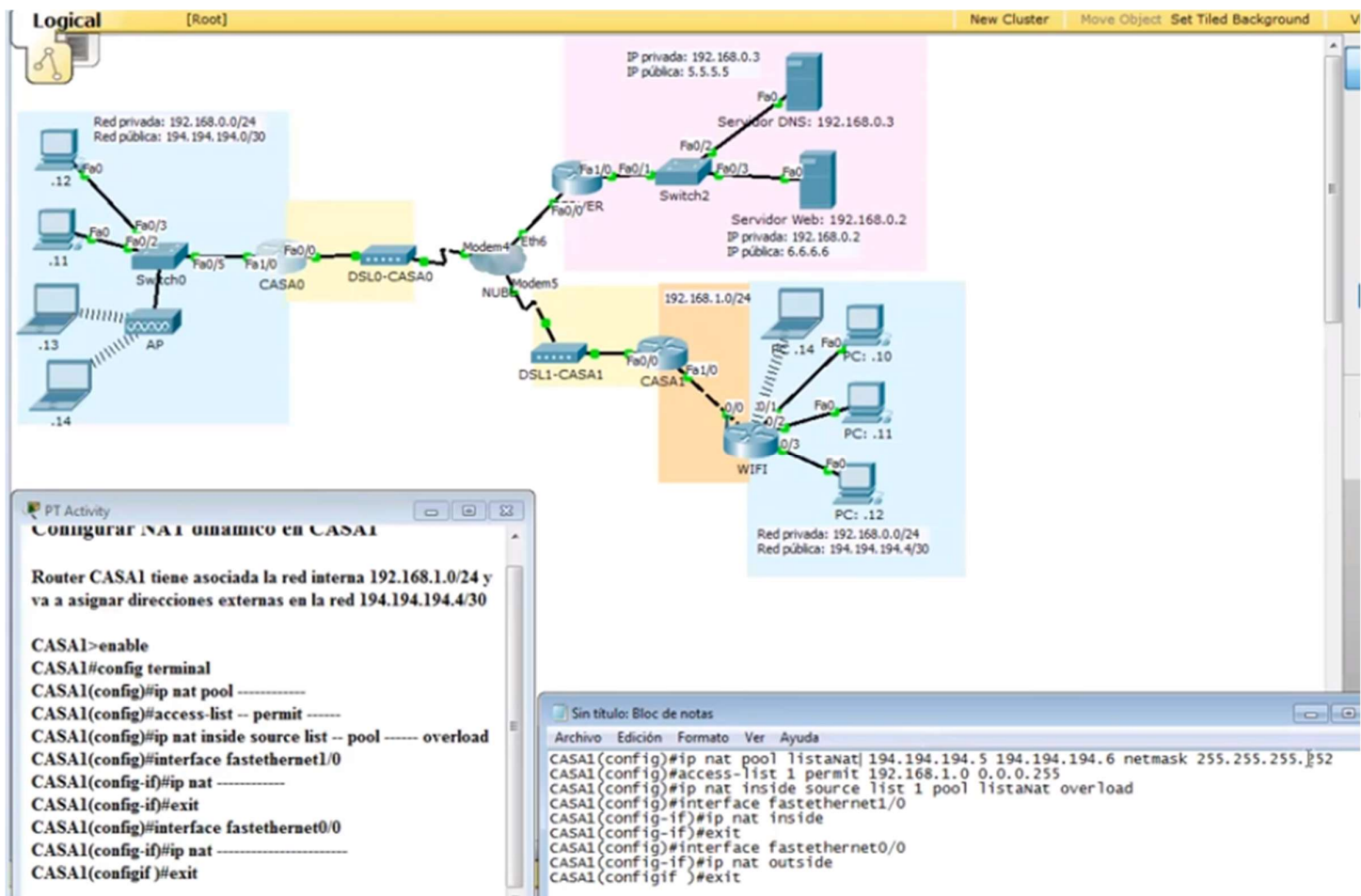
Router SEVER debe configurar Servidor web (IP interna: 192.168.0.2 e IP externa: 6.6.6.6) y Servidor DNS (IP interna: 192.168.0.2 e IP externa: 5.5.5.5)

```
SERVER>enable
SERVER#config terminal
SERVER(config)#ip nat inside source static 192.168.0.2 6.6.6.6
SERVER(config)#ip nat inside source static 192.168.0.3 5.5.5.5
SERVER(config)#interface fastethernet1/0
SERVER(config-if)#ip nat inside
SERVER(config-if)#exit
SERVER(config)#interface fastethernet0/0
SERVER(config-if)#ip nat outside
SERVER(config-if)#exit
```

Configurar NAT dinámico en CASA0

Router CASA0 tiene asociada la red interna 192.168.0.0/24 y va a asignar direcciones externas en la red 194.194.194.0/30 (seria mascara 255.255.255.252)

```
CASA0>enable
CASA0#config terminal
CASA0(config)#ip nat pool listaNat 194.194.194.1 194.194.194.2 netmask 255.255.255.252
CASA0(config)#access-list 1 permit 192.168.0.0 0.0.0.255 (MASCARA INVERTIDA)
CASA0(config)#ip nat inside source list 1 pool listaNat overload
CASA0(config)#interface fastethernet1/0
CASA0(config-if)#ip nat inside
CASA0(config-if)#exit
CASA0(config)#interface fastethernet0/0
CASA0(config-if)#ip nat outside
CASA0(config-if)#exit
```



CASAl#show ip nat statistics

Configuración DHCP en router

1) Indicar rango de IP excluido del pool (conjunto)

Router(config)#ip dhcp excluded-address [IP inicial] [IP final]

2) Asignar un nombre al conjunto de direcciones que serán asignadas.

Router(config)#ip dhcp pool [nombre]

3) Definir los parámetros.

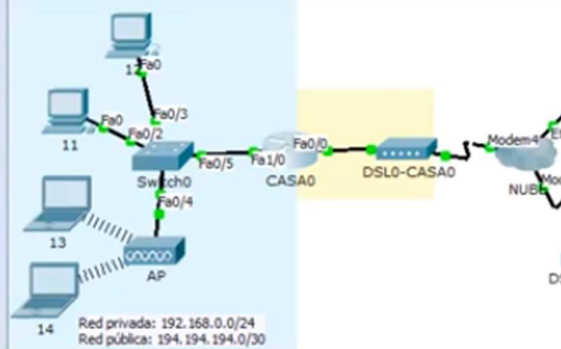
Router(dhcp-config)#network [IP RED] [MASCARA DE RED]

Router(dhcp-config)#default-router [IP routes]

Router(dhcp-config)#dns-server [IP servidor DNS]

Para mostrar tabla de asignación:

Router#show ip dhcp binding



```

PT Activity
direcciones 192.168.0.1 192.168.0.9
La red se llama RED_CASA0
Gateway: 192.168.0.1
Sevidor DNS: 5.5.5.5

CASA0>enable
CASA0#config terminal
CASA0(config)#ip dhcp excluded-address 192.168.0.1
192.168.0.9
CASA0(config)#ip dhcp pool RED_CASA0
CASA0(dhcp-config)#network 192.168.0.0 255.255.255.0
CASA0(dhcp-config)#default-router 192.168.0.1
CASA0(dhcp-config)#dns-server 5.5.5.5
CASA0(dhcp-config)#exit

```

```

PT Activity
Router CASA1 va a reservar (excluir) el rango de
direcciones 192.168.1.1 192.168.1.1
La red se llama RED_CASA1
Gateway: 192.168.1.1
Sevidor DNS: 5.5.5.5

CASA1>enable
CASA1#config terminal
CASA1(config)#ip dhcp excluded-address ---
CASA1(config)#ip dhcp pool RED_CASA1
CASA1(dhcp-config)#network -----
CASA1(dhcp-config)#default-router
CASA1(dhcp-config)#dns-server 5.5.5.5
CASA1(dhcp-config)#exit

```

Red privada: 192.168.0.0/24
Red pública: 194.194.194.4/30

```

Sin título: Bloc de notas
Archivo Edición Formato Ver Ayuda

CASA1>enable
CASA1#config terminal
CASA1(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.1
CASA1(config)#ip dhcp pool RED_CASA1
CASA1(dhcp-config)#network 192.168.1.0 255.255.255.0
CASA1(dhcp-config)#default-router 192.168.1.1
CASA1(dhcp-config)#dns-server 5.5.5.5
CASA1(dhcp-config)#exit

```

TDIII - Práctico: DHCP

Tenemos un sistema de redes (con las mismas direcciones IP en los host)

Las direcciones IP privadas en las redes son:

- * CASA0: 192.168.0.0/24
- * CASA1 tiene dos redes 192.168.1.0/24 y 192.168.0.0/24
- * SERVER: 192.168.0.0/24

Las direcciones IP públicas para cada red son:

- * CASA0: 194.194.194.0/30
- * CASA1: 194.194.194.4/30
- * SERVER: 6.6.6.6 y 5.5.5.5

La red esta configurada, de la siguiente forma: Host con direcciones IP, máscara, gateway, servidor DNS por DHCP Routers: con NAT y rutas estáticas configuradas

Configurar servidor DHCP en router CASA0

Router CASA0 va a reservar (excluir) el rango de direcciones 192.168.0.1 192.168.0.9

La red se llama RED_CASA0

Gateway: 192.168.0.1

Sevidor DNS: 5.5.5.5

```
CASA0>enable
```

```
CASA0#config terminal
```

```
CASA0(config)#ip dhcp excluded-address 192.168.0.1 192.168.0.9
```

```
CASA0(config)#ip dhcp pool RED_CASA0
```

```
CASA0(dhcp-config)#network 192.168.0.0 255.255.255.0
```

```
CASA0(dhcp-config)#default-router 192.168.0.1
```

```
CASA0(dhcp-config)#dns-server 5.5.5.5
```

```
CASA0(dhcp-config)#exit
```

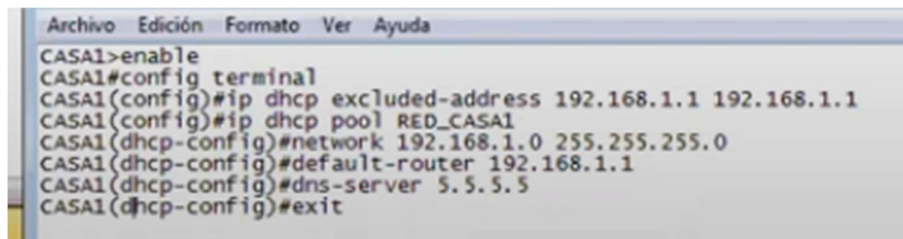
Configurar servidor DHCP en router CASA1

Router CASA1 va a reservar (excluir) el rango de direcciones 192.168.1.1 192.168.1.1

La red se llama RED_CASA1

Gateway: 192.168.1.1

Sevidor DNS: 5.5.5.5



```
Archivo Edición Formato Ver Ayuda
CASA1>enable
CASA1#config terminal
CASA1(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.1
CASA1(config)#ip dhcp pool RED_CASA1
CASA1(dhcp-config)#network 192.168.1.0 255.255.255.0
CASA1(dhcp-config)#default-router 192.168.1.1
CASA1(dhcp-config)#dns-server 5.5.5.5
CASA1(dhcp-config)#exit
```

Configurar servidor DHCP Linksys en red CASA1

Configuración Interfaz Internet: DHCP

Vemos como se relean los campos.

Configuración Interfaz LAN: IP 192.168.0.1/24

Configurar servidor DHCP Linksys en red CASA1

En GUI vamos a Setup:

IP router 192.168.0.1 /24

Habilitamos servidor DHCP

Guardar configuración

Dirección IP inicial 192.168.0.20

Número máximo de usuarios 100

DNS estático: 5.5.5.5

Guardar configuración

Verificación:

Para mostrar tabla de asignación Router CASA0:

```
CASA0>enable
```

```
CASA0#show ip dhcp binding
```

