

Actividad 0. [1,5 puntos]

Indica las diferencias entre un switch/conmutador FastEthernet, un hub/concentrador FastEthernet y un Punto de Acceso Wi-Fi 802.11n, con respecto a:

1. El **ancho de banda** siempre disponible para cada estación conectada (pon ejemplos)

Los switch son los únicos dispositivos de red de los tres mencionados en el enunciado que son capaces de proporcionar el máximo ancho de banda en todo momento para todas las estaciones conectadas a ellos. El switch es capaz de identificar las estaciones concretas que ha de comunicar gracias a la dirección MAC (almacena dicha información en sus tablas MAC), crea canales de comunicación directa entre ambas estaciones, permitiendo el uso completo del ancho de banda.

Tanto un concentrador HUB como un punto de acceso inalámbrico carecen de esta capacidad, en ambos casos aunque el medio sea distinto (cable en el caso del concentrador y ondas radiofónicas en el caso del punto de acceso) estos dispositivos reenvían la información recibida de una de las estaciones a todas las demás conectadas a ellos, y dichas estaciones son las encargadas de comprobar si los paquetes que están recibiendo son para ellas y aceptarlos, o van dirigidos a otra estación y desecharlos. Esto hace que en la práctica el ancho de banda sea compartido en todo momento por todas las estaciones independientemente de cuáles se estén comunicando entre sí.

2. Las **capas** en que trabajan principalmente y qué hacen en cada capa.

Switch: El conmutador trabaja en la capa de enlace de datos capaz de crear dominios de colisión. Es un dispositivo capaz de identificar y almacenar en sus tablas internas la dirección MAC de los dispositivos de red conectados a cada uno de sus puertos. De esta forma el switch es capaz de crear canales de comunicación directos entre dos estaciones de trabajo.

HUB: Por otro lado el hub trabaja al nivel de la capa física y no es capaz de crear dominios de colisión. Es un dispositivo muy simple que funciona a modo de repetidor, difundiendo la información que llega por alguno de sus puertos hacia todos los demás.

Punto de acceso inalámbrico: Este dispositivo trabaja al igual que el switch en la capa de enlace de datos. Es capaz de generar dominios de colisión, y es capaz de identificar las direcciones MAC de origen y destino de los paquetes. No obstante dada la idiosincrasia de su medio de transmisión (ondas radiofónicas omnidireccionales) el punto de acceso no puede crear canales de comunicación directos entre 2 estaciones, todas las conectadas al punto de acceso recibirán el paquete y lo aceptarán o descartarán si va dirigido o no a su propia MAC.

3. Cómo gestionan las **colisiones (nombra protocolos, casos que aplican según dúplex, etc.)**

Switch: El switch crea comunicaciones directamente entre los puertos correspondientes de los nodos implicados. Si otras estaciones están intentando transmitir a la vez, el switch simplemente almacena los paquetes en un buffer y los transmite a su destino en secuencia ordenada una vez sea posible. Por tanto con un switch, no se producen colisiones.

Hub: Dado que el hub simplemente repite toda la información que recibe por un puerto, a al resto de puertos, las colisiones son muy probables. Para solucionar el problema, existen protocolos que usan los distintos nodos conectados a la red, para minimizar y solucionar las colisiones.

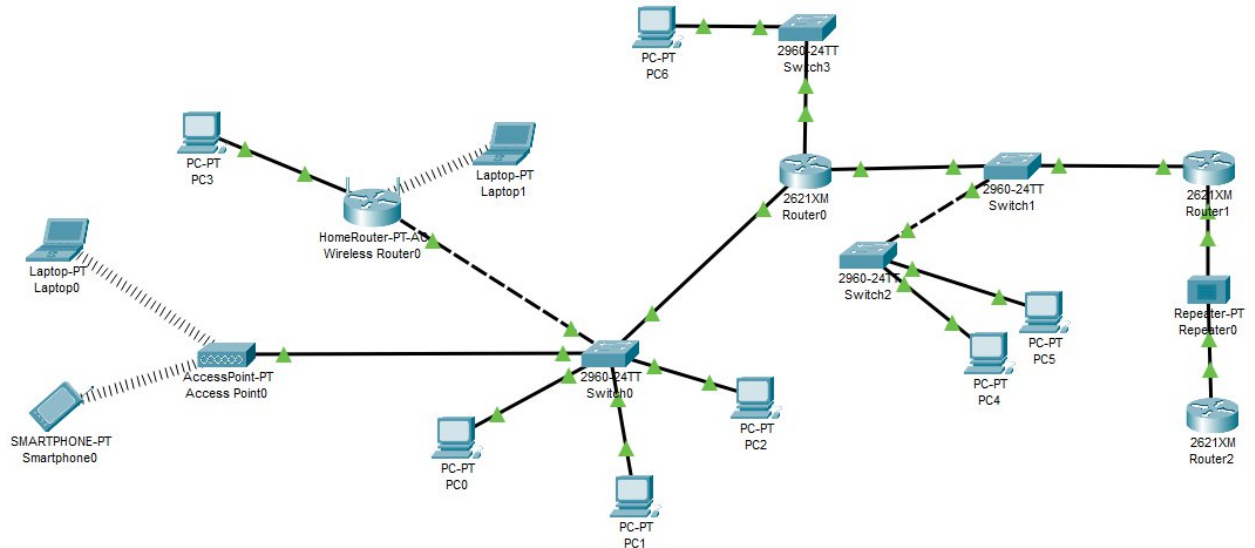
En conexiones ethernet no duplex, solía usarse CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance). Este protocolo hace que los nodos escuchen el medio antes de transmitir. Si el medio esta libre, se transmite, si esta ocupado se espera una cantidad de micro segundos aleatoria y se vuelve a intentar la transmisión tras escuchar nuevamente el medio. Este protocolo solo trata de evitar las colisiones, no aporta ninguna solución si estas se producen.

En conexiones full duplex, se usa principalmente la variante CSMA/CD (Carrier Sense Multiple Access/Collision Detect). Con este protocolo, se pretende que los dispositivos de la red, sean capaces de identificar cuando se ha producido una colisión, y solicitar al otro dispositivo que repita el mensaje que se ha perdido durante dicha colisión.

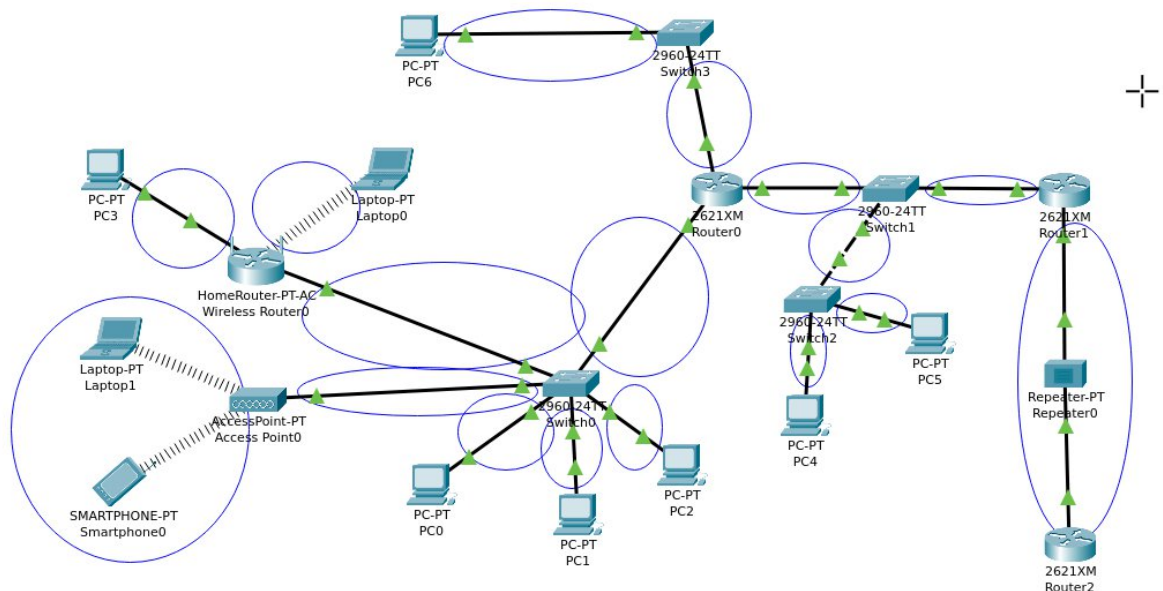
Punto de acceso inalámbrico 802.11: En las redes WLAN, la problemática es similar a la de un hub, por lo que se usan el protocolo CSMA/CA. Sin embargo el protocolo CSMA/CA no resuelve por si solo problemáticas específicas de la red WLAN como el “problema del nodo oculto”, que se da cuando dos nodos de la red están a distancia suficiente para no ser capaz de detectarse entre ellos (y por tanto coordinarse para la transmisión), pero si son capaces de conectar con el punto de acceso. Para solucionar esta problemática, se creo la extensión del protocolo CSMA/CA RTS/CTS (Request To Send/Clear To Send), que hace que los nodos pidan previamente permiso para retransmitir al punto de acceso, y si el medio esta libre se les concede el permiso para transmitir.

Actividad 1. [2 puntos]

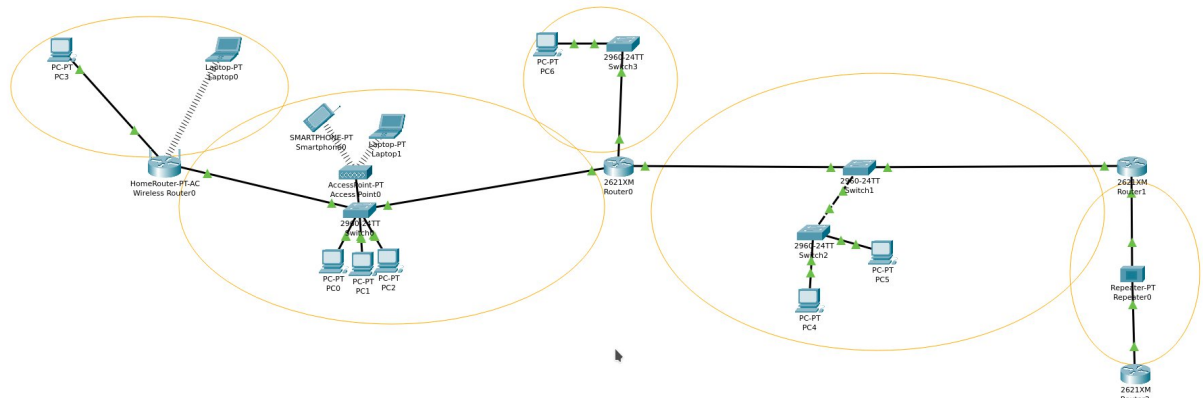
Examina detalladamente la figura que representa una red corporativa. Crea un esquema de red similar en **Packet Tracer** y responde a las siguientes preguntas justificando claramente tu respuesta:



1. ¿Cuántos **dominios de colisión** existen en esta red? Dibújalos sobre el diagrama de red con la herramienta Elipse de PT (tecla E) de color **AZUL** y adjunta una captura de pantalla.



2. ¿Cuántos **dominios de difusión** habría (suponiendo que se asignan las diferentes subredes IP en los diferentes dominios de difusión)? Dibújalos sobre el diagrama de red con la herramienta Elipse de PT de color **NARANJA** y adjunta una captura de pantalla.



3. ¿Qué dispositivos de la figura son capaces de separar/crear diferentes dominios de colisión?

En la figura, los dispositivos capaces de crear o separar distintos dominios de colisión serían los switches, los routers (incluye los router normales y el domestico) y la interfaz ethernet del punto de acceso alámbrico (si bien el AP wireless funciona en la capa 2, las redes inalámbricas son un medio compartido por definición y funcionan como un único dominio de colisión)

¿y de difusión?

Los routers son los únicos que pueden crear dominios de difusión. En este caso tanto los normales como el domestico. Depende de como consideremos a este ultimo, también podríamos decir que es un switch con funcionalidades de enrutamiento y que por tanto es un conmutador con capacidad de crear dominios de difusión.

4. ¿Llegaría una trama MAC de difusión desde el Smartphone0 hasta el PC2? ¿Por qué?

Si, ambos terminales se encuentran en el mismo dominio de difusión, en la misma red o subred y por tanto son capaces de recibir las tramas de difusión enviadas por el otro dispositivo.

Y desde el Laptop1 hasta el PC6, ¿llegaría una trama MAC de difusión? ¿Por qué?

No, este es el caso contrario. Los dispositivos se encuentran en redes o subredes distintas, con uno o varios routers por el camino, por lo que pertenecen a dominios de difusión diferentes. Para que un paquete pueda llegar de un dispositivo a otro, es necesario que los router encaminen el paquete mediante IP en la capa de red, y eso ya no sería una trama de difusión.

Actividad 2. [2 puntos]

Dado el anterior diagrama de red.

DNI:45885499q

Suponiendo que solo nos permiten usar el rango de direcciones 130.99.0.0 /21 para toda la red.

Siendo: X las 2 últimas cifras de tu NIF, salvo si es 00 que tendrás que poner un 01

Y que se quiere dimensionar la red para que soporte como máximo:

- 50 equipos conectados al Access Point0 y 64 equipos al Switch0
- 250 equipos conectados al WirelessRouter0 (juntando WiFi y cableados)
- 24 equipos conectados al Switch1 y otros 20 al Switch2
- 120 equipos conectados al Switch3.

a) Segmenta en diferentes subredes de una forma eficiente (sin desperdiciar IPs). Realiza una tabla con información detallada para cada tramo/segmento de red/subred.

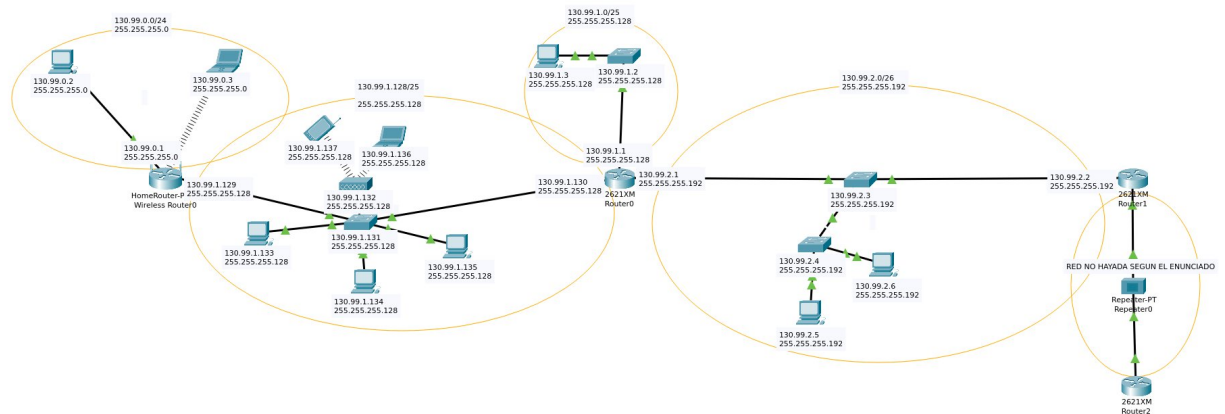
Host solicitados	Bits necesarios para host	Host disponibles	Direccion de red	Mascara de red	1ºIP disponible	Ultima IP disponible	Broadcast
250	8	254	130.99.0.0	255.255.255.0	130.99.0.1	130.99.0.254	130.99.0.255
124	7	126	130.99.1.0	255.255.255.128	130.99.1.1	130.99.1.126	130.99.1.127
114	7	126	130.99.1.128	255.255.255.128	130.99.1.129	130.99.1.254	130.99.1.255
44	6	62	130.99.2.0	255.255.255.192	130.99.2.1	130.99.2.62	130.99.2.63

b) Dibuja e indica en el diagrama de red :

- las diferentes direcciones de subred (con su máscara correspondiente). Una por de cada "Elipse Naranja".
- las direcciones IP+máscara a asignar a cada uno de los equipos de red.
- Si un router tiene varios interfaces en diferentes subredes (o dominios de difusión) necesitará una IP diferente en cada una de las subredes
- Los equipos que trabajan a nivel 1 y/o 2 como el Repetidor, Access Point y Switches, también necesitarán una IP asignada para poder administrarlos/gestionarlos remotamente.

Usa la herramienta de Notas de Packet Tracer (tecla N) para etiquetar las IPs+Máscaras. Pero no es necesario que las configures en los equipos.

Nota: En general los dominios de difusión calculados anteriormente se corresponderán con las distintas **subredes IP a nivel 3**. Hay que tener en cuenta esto a la hora de diseñar el direccionamiento IP. También es importante que vayas reservando primero los rangos más grandes (con más equipos a asignar direcciones) y les vayas reservando los rangos desde los más altos a los más bajos.



Actividad 3. [2 puntos]

Usando PT y entrando al CLI (Command Line Interface) del Switch0.

Escribe los comandos que necesitamos teclear en el orden adecuado para que:

1. El nombre del switch sea [TuApellido]PAR03.

```
Switch0 <@Bt-Standard-PC-Q35-ICH9-2009>
Physical Config CLI Attributes
IOS Command Line Interface
Model number: WS-C2960-24TT-L
System serial number: FOC1680304
Top Assembly Part Number: 800-27221-02
Top Assembly Revision Number: A0
Version ID: V02
OLEI Code Number: C00L0000A
Hardware Board Revision Number: 0001
Switch Ports Model SW Version SW Image
-----
* 24 WS-C2960-24TT-L 15.0(2)SE4 C2960-LANBASEK9-M
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled wed 26-Jun-13 02:40 by engineers

Press RETURN to get started!

NLINK-S-CHANGED: Interface FastEthernet0/2, changed state to up
NLINKPROTO-S-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
NLINK-S-CHANGED: Interface FastEthernet0/2, changed state to up
NLINKPROTO-S-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
NLINK-S-CHANGED: Interface FastEthernet0/3, changed state to up
NLINKPROTO-S-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
NLINK-S-CHANGED: Interface FastEthernet0/4, changed state to up
NLINKPROTO-S-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up
NLINK-S-CHANGED: Interface FastEthernet0/5, changed state to up
NLINKPROTO-S-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up
NLINK-S-CHANGED: Interface FastEthernet0/6, changed state to up
NLINKPROTO-S-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up

Switch>clear
Translating "clear"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address

Switch>enable
Switch>configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname CarrascoPAR03
Switch(config)#
```

Unidad 3 Guía: Configuración de Conmutadores

Con lo que nuestra pantalla quedará

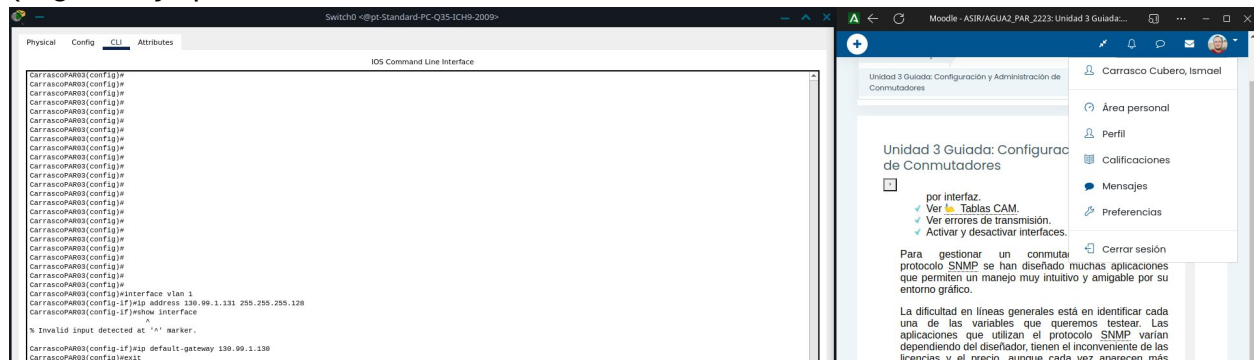
```
switch(config)#
```

A partir de aquí podemos empezar a cambiar parámetros, por ejemplo, el nombre de nuestro switch lo cambiamos con el comando hostname:

```
switch(config)# hostname ALISAL
ALISAL(config)#
```

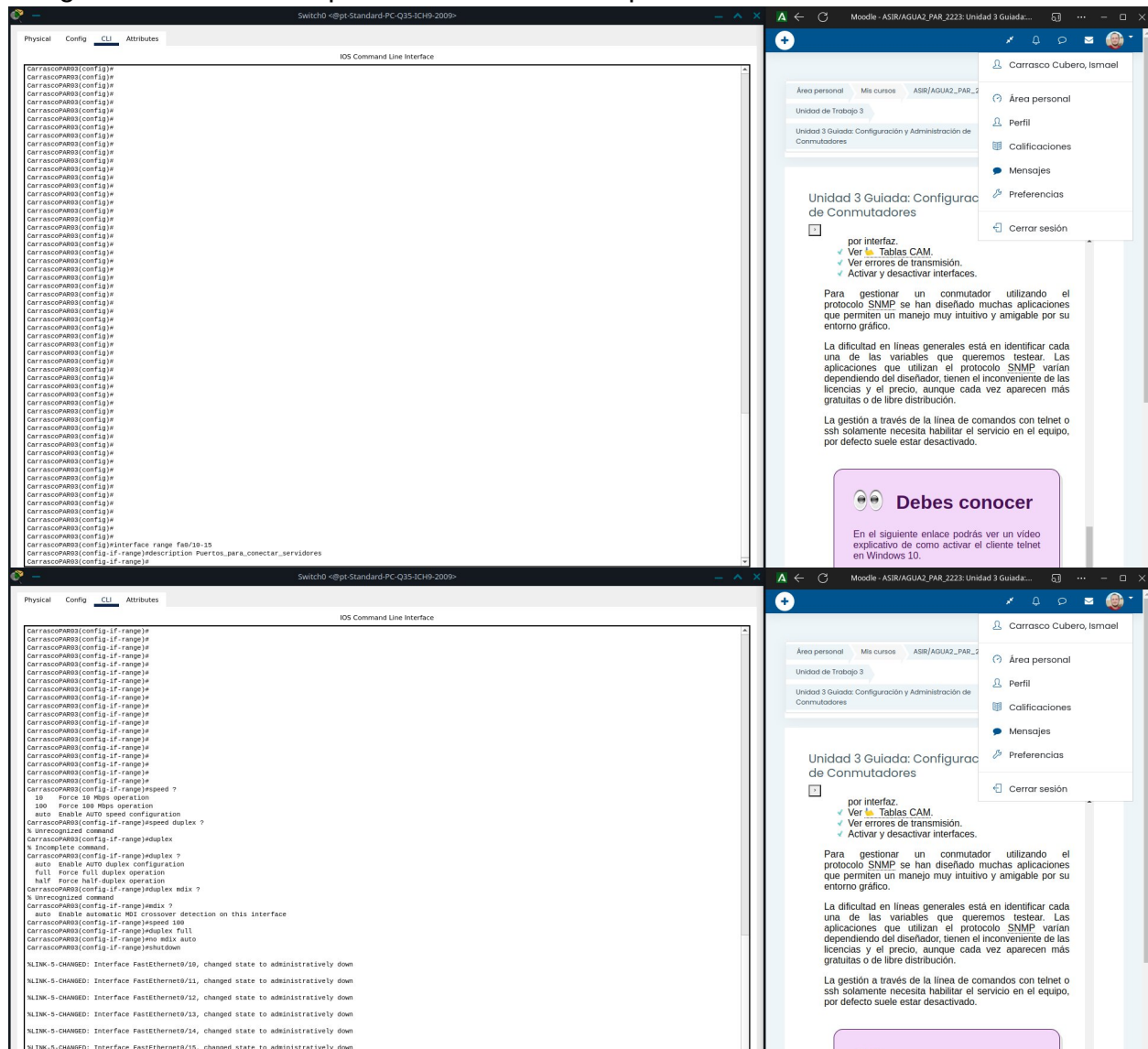
Y podríamos comenzar a ejecutar órdenes de configuración en nuestro conmutador. Si utilizamos la vía Web o una aplicación gráfica basada en SNMP, el proceso sería más intuitivo, basado en un sistema de ventanas.

1. Configurarle una dirección IP y máscara según lo calculado en la anterior actividad. Y configura la dirección IP de la puerta de enlace predeterminada (el *gateway* que debe ser la IP del Router0).

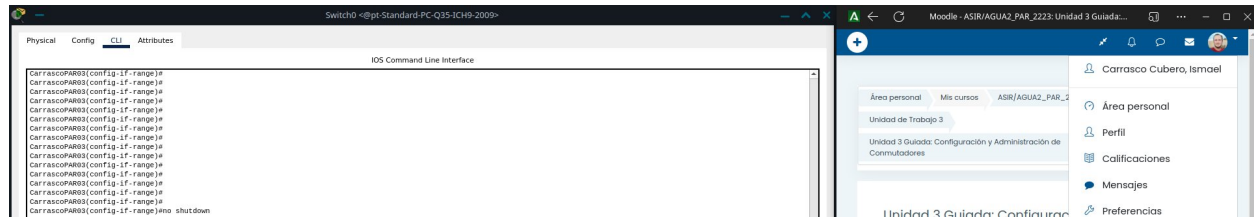


1. Usando la documentación de los enlaces de la "Información de Interés" de la tarea, configura el rango de puertos FastEthernet desde 10 al 15 del módulo 0 para que:

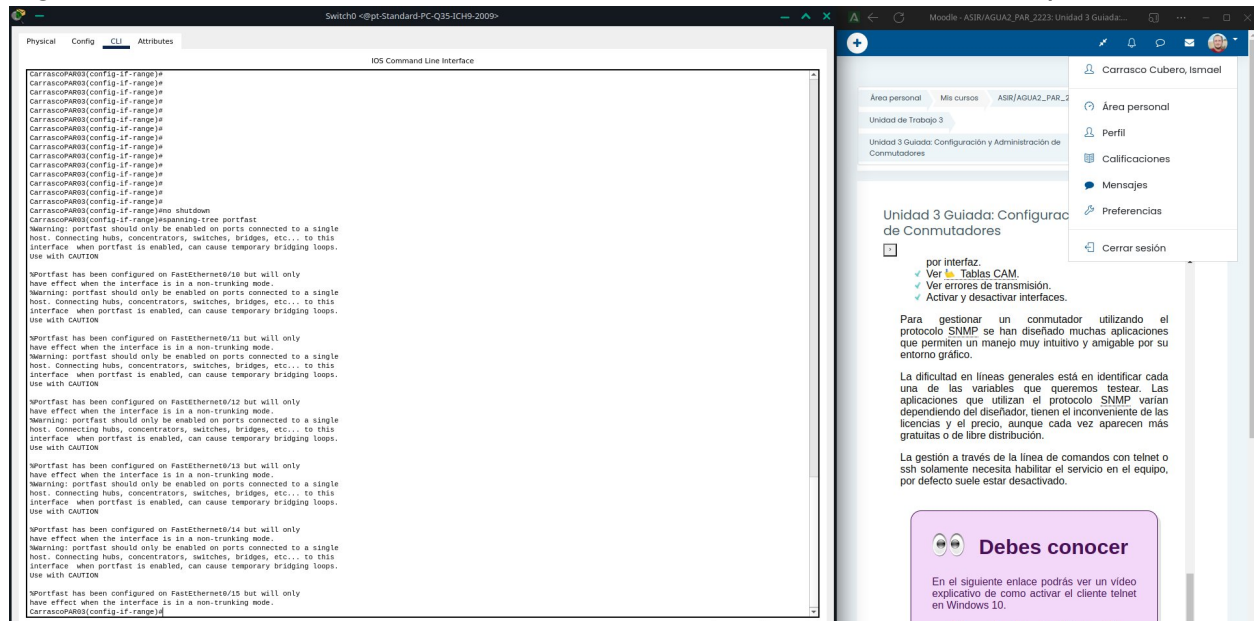
1. Tengan la descripción "Puertos para conectar servidores"



1. Se desactiven y se vuelvan a activar los puertos para reiniciarlos.



1. Configura en ese mismo rango de puertos el comando "*spanning-tree portfast*". Investiga y explica para qué sirve, y si tiene algún efecto en la velocidad de reinicio de los puertos. Compruébalo reiniciándolos poniendo algún PC conectado a alguno de esos puertos.



La funcionalidad de portfast, permite que un puerto recién conectado, se salte los estados de listening y learning, y pase directamente al estado de forwarding, por lo que la conexión con el equipo conectado a ese puerto se establece de forma mucho mas rápida. En el caso del equipo con el que he realizado la prueba, apagando el puerto y volviendo a encenderlo, la conexión se realizaba de forma prácticamente instantánea.

Actividad 4. [2,5 puntos]

Añade 2 switches (Switch4 y Switch5) Cisco 2960 conectados a Switch3 formando un anillo.

Une switch3 y switch4 mediante un enlace de **GigaEthernet**.

Une switch3 con switch5 mediante el puerto **FastEthernet0/10** en ambos switches.

Une switch4 con switch5 mediante **GigaEthernet**.

Añade el PC7 al Switch3.

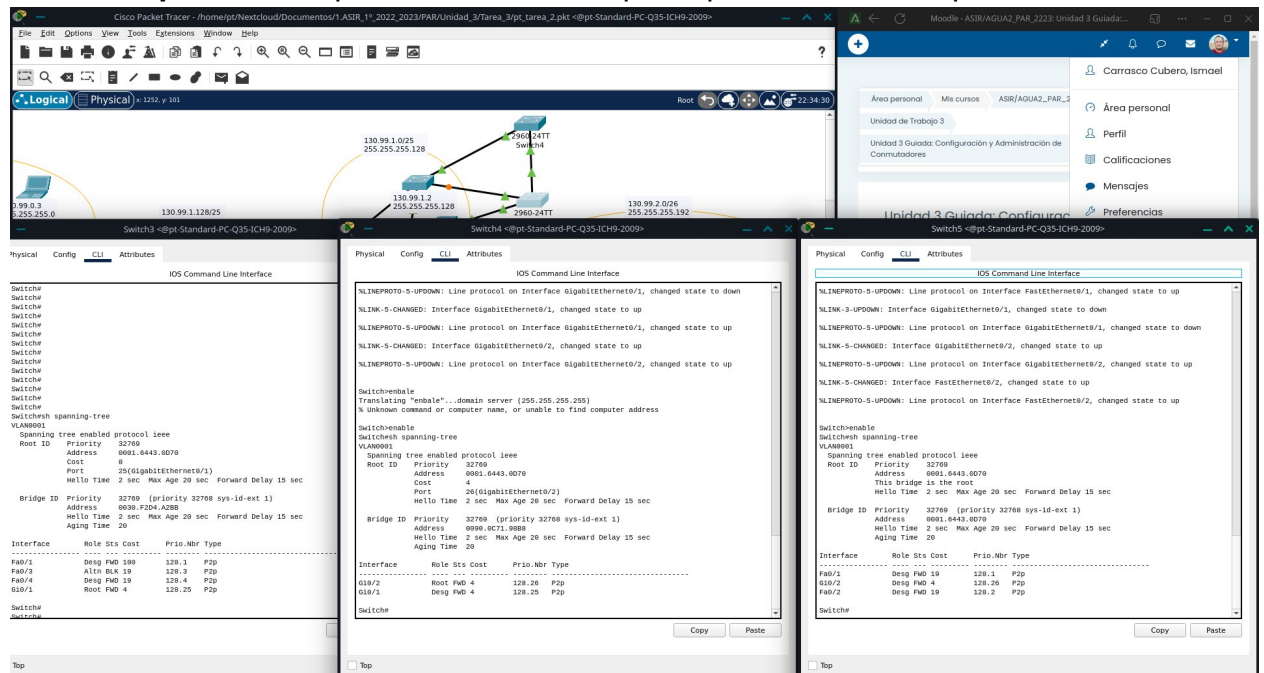
Asigna IP+máscara a PC6 y PC7 según corresponda en la actividad 2.

Cambia PC6 para que esté conectado al Switch5.

a) root del STP (raíz del Spanning-Tree)

Muestra una captura de pantalla dónde se vea la salida del comando necesario para saber quien es el root del spanning-tree. Explica brevemente por qué crees que se ha elegido ese root.

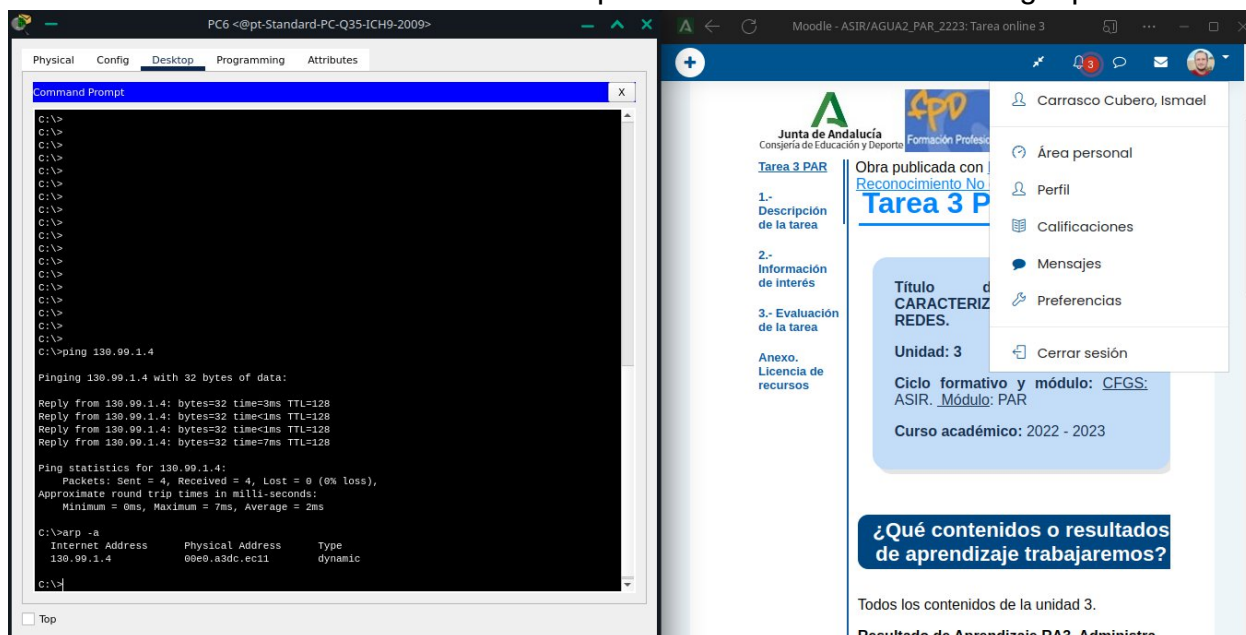
Muestra otra captura dónde se vea si hay algún interfaz de algún switch en modo **bloqueado**. Explica brevemente por qué se ha bloqueado ese interfaz



En la captura anterior, se puede apreciar la respuesta a ambas preguntas. Vemos que se ha elegido como root del spanning-tree a switch5. Al estar conectados en anillo, cualquiera podría ser el root, en este caso el protocolo STP ha acordado que switch5 sea el root por tener la dirección MAC mas baja.

También se puede apreciar que el puerto fast ethernet 3 del switch 3 esta en estado bloqueado y a adquirido el rol de vía alternativa. Dado que el resto de conexiones entre los switches del spanning tree son via Gigabit ethernet, este puerto se bloquea para evitar que el forwarding tome la vía mas lenta, quedando reservado como camino alternativo por si las otras conexiones fallan.

b) ¿Cómo puede un usuario conectado a PC6 conocer la MAC del PC7? Muestra y comenta las capturas con el comando para saber la dirección MAC de PC7 desde PC6 sabiendo la dirección IP de PC7. Y explica si necesitarás hacer algo previamente.



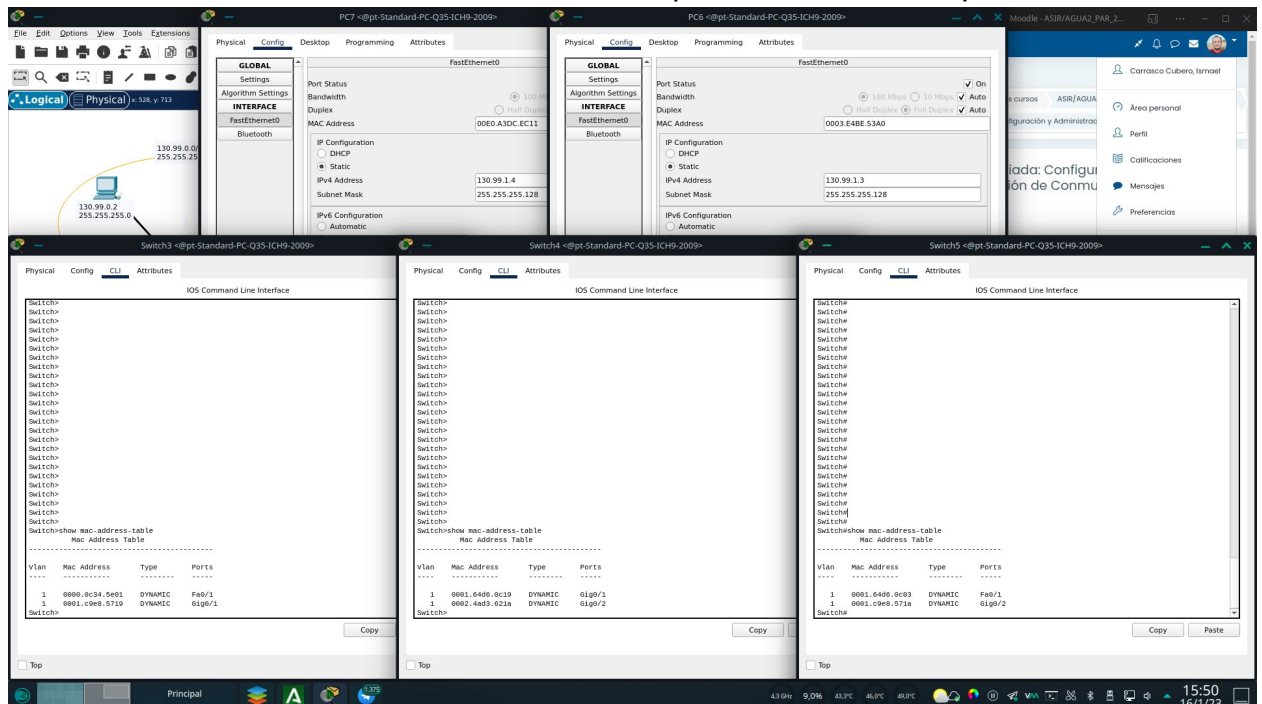
Se puede mostrar la dirección IP del PC06 desde el command prompt de PC07 usando el comando arp -a para mostrar las entradas de la tabla arp, con sus direcciones IP asociadas a sus correspondientes MAC. Si no hacemos nada, el comando nos informara de que no hay entradas en la tabla. Para solucionar eso, podemos simplemente lanzar un ping desde PC06 a PC07 ya que sabemos su IP. Una vez que PC07 responda a PC06, este almacenara la dirección MAC de origen en su tabla ARP para futuras conexiones y podremos verla con el comando arp -a. Se puede ver el proceso en la captura superior.

c) ¿Cómo aprende el switch dónde está cada MAC de destino? Explica brevemente cómo es el funcionamiento “**plug&play**” de un switch. ¿Cómo aprende los equipos que tiene conectados en cada interfaz/puerto? ¿Qué hace al arrancar y qué hace una vez que completa su tabla de MACs?

El proceso se realiza gracias al protocolo de resolución de direcciones ARP (Address Resolution Protocol). Cuando un conmutador se enciende comienza a comprobar cuales de sus puertos tienen algún dispositivo conectado y comienza a enviarles paquetes de tipo ARP request, los cuales indican al dispositivo conectado en el puerto que deben enviar un paquete de tipo ARP reply indicando cual es su dirección MAC. Con dicha información, el conmutador construye una tabla ARP en la que asocia direcciones MAC a cada uno de los puertos, para poder redirigir el trafico a su destino.

Una vez lista la tabla, si el conmutador recibe un paquete con una dirección MAC desconocida como destino con una IP asociada (por ejemplo, se ha conectado un nuevo dispositivo al conmutador), este enviara una trama ARP por todos los puertos (flooding) excepto el de origen, para que la maquina de destino responda con su dirección física (el resto lo descartaran). Al obtener respuesta de la maquina de destino, el conmutador puede aprender que en dicho puerto se encuentra la nueva MAC, y añade la correspondiente entrada a la tabla ARP.

d) Muestra y comenta las capturas necesarias para saber por qué camino (a nivel de capa de enlace/físico) iría un ping desde PC6 a PC7. Debes hacerlo sin usar la herramienta “simulación” de Packet Tracer. Solo puedes usar comandos en los switches desde el modo en “Tiempo Real” para mostrarlo.

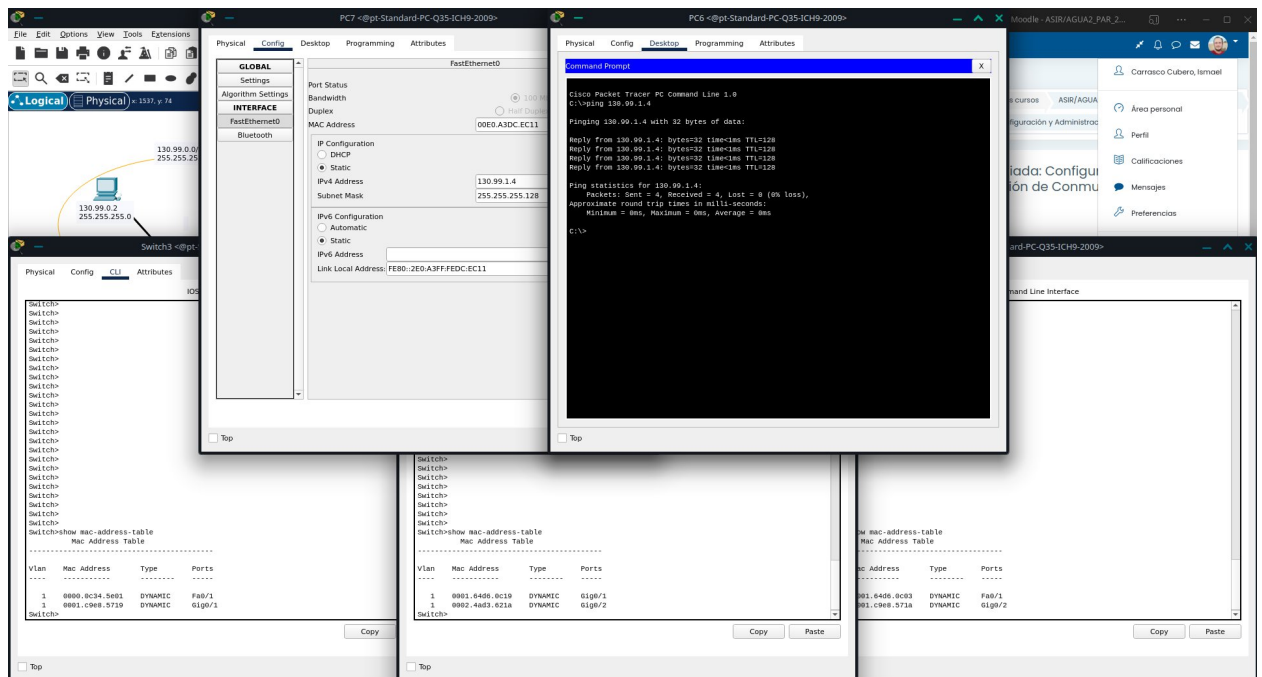


Si visualizamos las tablas mac de los 3 conmutadores con el comando show mac-address-table, con la simulación recién iniciada, podemos comprobar que las únicas entradas que constan en las tablas de los conmutadores son las direcciones mac de los otros dos conmutadores conectados a ellos:

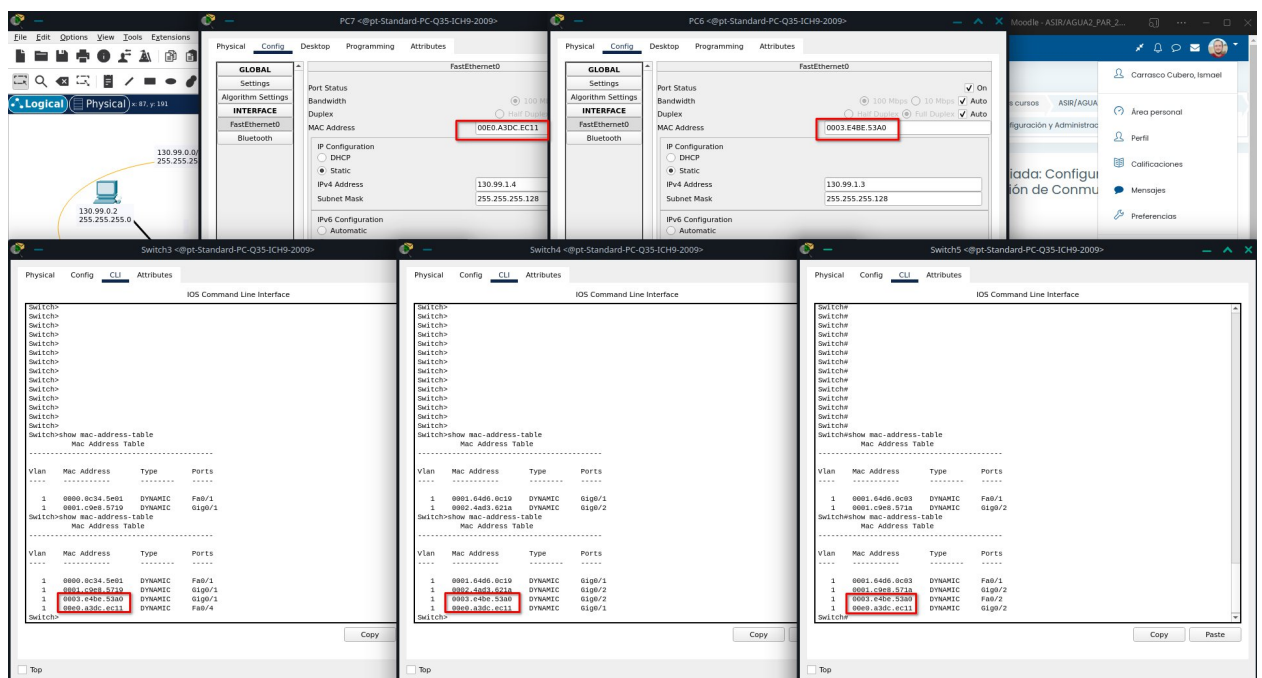
En switch3: se muestran switch4 y switch5

En switch:4 se muestran switch3 y switch5

Y en switch5: se muestran switch 3 y switch4



Tras eso procedemos a ejecutar un ping desde el pc06 al pc07.



Tras lo cual, vemos que a las tablas MAC de los switches se han añadido dos nuevas entradas, tanto las del pc06 como las del pc07.

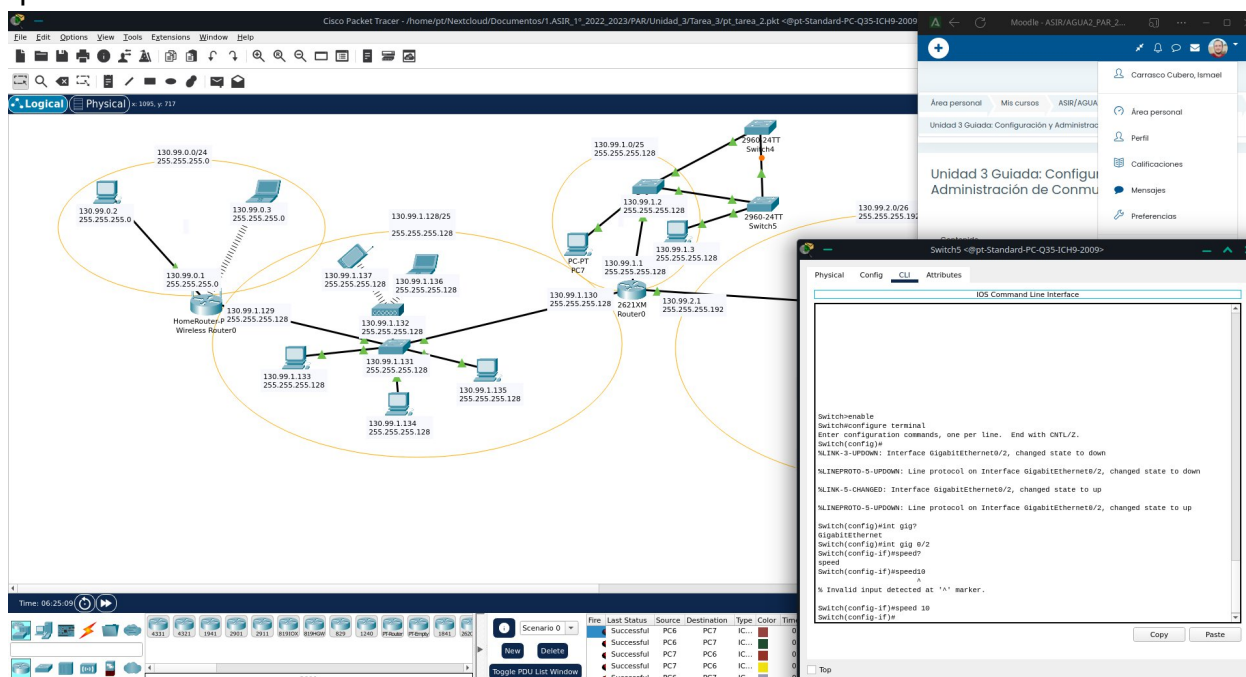
Dado que pc06 está conectado a switch5, y que las entradas en las tablas MAC constan en los 3 switches, la única conclusión lógica es que la solicitud ping ha recorrido los 3 switches de forma secuencial (s5, s4 y s3) escogiendo la ruta de los puertos gigabit, hasta llegar al pc07 para luego la respuesta recorrer de nuevo el mismo camino de forma inversa.

e) STP tras cambio de velocidad

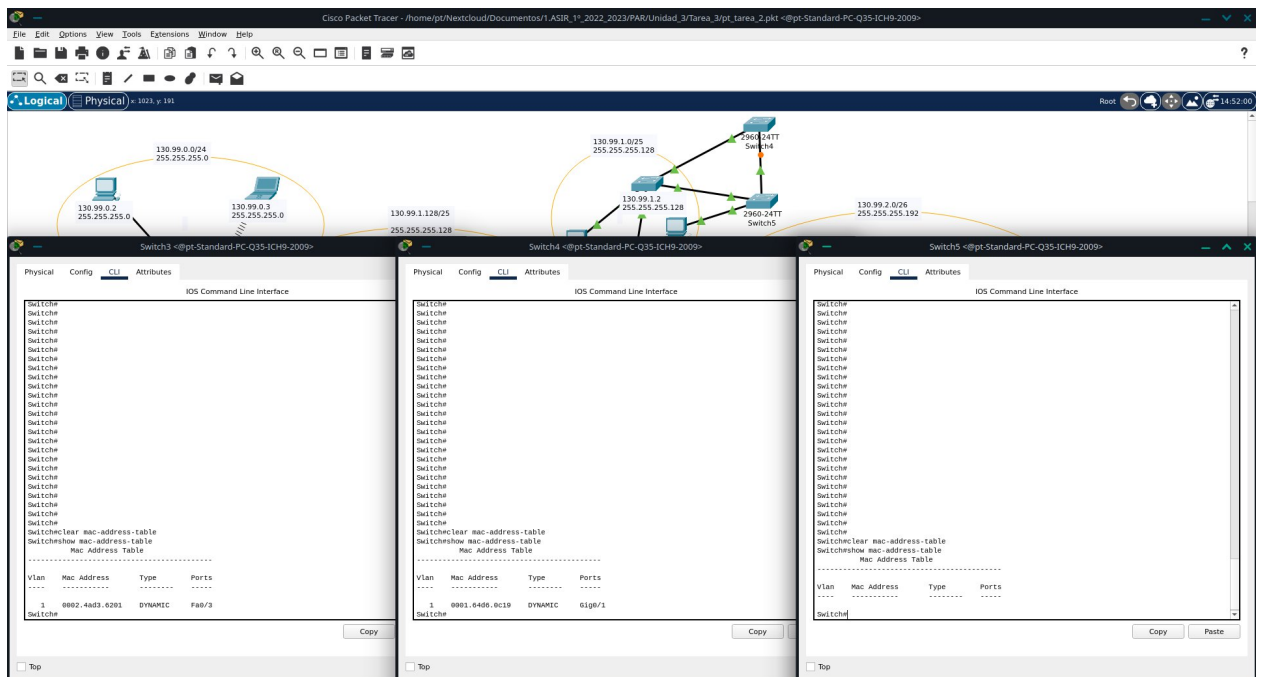
Pon en el switch5 una velocidad de 10Mbps al interfaz de Giga que conecta con el switch4. Reinicia el enlace y explica qué ocurre con el Spanning-tree mostrando capturas y explicando lo que ha pasado.

Muestra y comenta las capturas necesarias para saber por qué camino iría ahora un ping desde PC6 a PC7. De nuevo solo puedes usar comandos desde el modo en “Tiempo Real”.

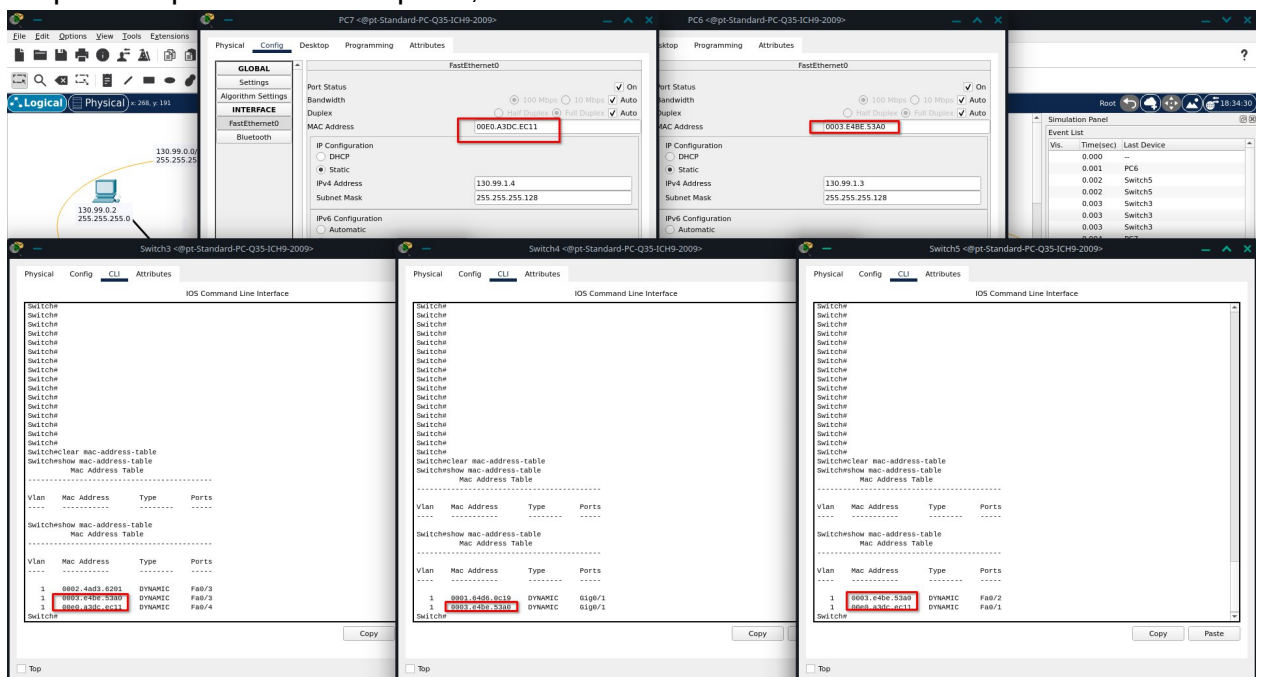
¿Con qué comando se puede **reiniciar la tabla de MACs** en un switch Cisco sin tener que reiniciarlo?



Entrando en la configuración de la interfaz y seleccionando la velocidad a 10megabits, con el comando "speed 10", podemos observar al cabo de unos segundos (no he necesitado ni tan siquiera reiniciar el enlace), como esa conexión entre ambos switches, antes activa ahora pasa a estado bloqueado. Se puede observar también que el puerto fast ethernet que antes estaba en estado bloqueado, comienza a cumplir su misión de vía alternativa y se activa automáticamente.



Con el comando “clear mac-address-table” se borran todas las entradas del switch, como se puede apreciar en la captura, si a continuación mostramos la tabla de MAC actual.




Tras realizar otro ping, y volver a mostrar las tablas MAC, observamos que ambos pc aparecen de nuevo en switch 5 y switch 3. Switch4 solo tiene almacenada la MAC de la maquina de origen, pero no la de destino. Esto nos indica que efectivamente la ruta ha cambiado y ahora los paquetes pasan de un host a otro, desde switch5 a switch3 ignorando a switch4.

Actividad 5. Opcional, pero será valorada en la calificación de los foros: Comenta en el foro e inserta en tu tarea las capturas de pantalla en las que se vea bien todo el texto con tus entradas en el foro. Por ejemplo:

- Algo que cambiarías o añadirías en algún apartado en concreto de los contenidos de la unidad.
- Referencia lo que dices con algún **enlace web** o **documento que adjuntes**.
- Puedes usar **Wikipedia** y la búsqueda por Internet de **materiales libres**.
- Alguna pregunta tipo test que puedas proponer según los contenidos vistos. Justifica la respuesta.
- Alguna otra propuesta de tarea o ejercicio que creas más interesante, o modificar alguno de los ejercicios.
- **Los enlaces web que te hayan sido útiles para resolver la tarea.**

Se valorará la creatividad, así que intentar no repetir lo que otros compañeros hayan comentado. Cuanto antes comentes tendrás más facilidad para no repetir.



Re: /* Propuestas preguntas tipo test - De la TAREA 3
de Carrasco Cubero, Ismael - lunes, 16 de enero de 2023, 19:29

Con que orden podemos cambiar a modo privilegiado en la CLI de un conmutador Cisco como el 2960?

- a) privileges
- b) enable**
- c) admin
- d) sudo

[Enlace permanente](#) [Marcar como no leído](#) [Mostrar mensaje anterior](#) [Editar](#) [Borrar](#) [Responder](#)

<https://educacionadistancia.juntadeandalucia.es/formacionprofesional/mod/forum/discuss.php?d=12165#p126317>

Autoevaluacion

Actividad 0: Creo que esta actividad la tengo razonablemente bien. Las explicaciones están justificadas y espero que al menos en buena parte correctas. 7,5 sobre 10?

Actividad 1: Mas o menos como la anterior, pero esta creo que esta algo mejor. He respondido a las preguntas y he justificado mis razonamientos. Puede que en los dominios de colisión y difusión alguno falte o sobre, pero creo que están mas o menos bien. 8 sobre 10?

Actividad 2: Esta no lo tengo claro, tengo la impresión de que conozco los fundamentos para realizar un subneteo variable con VLSM, pero como es algo tan complejo siempre me deja inseguro. Siendo conservador 6,5 sobre 10?

Actividad 3: Esta considero que esta bastante bien. He realizado todos los puntos y he adjuntado capturas de todos los procesos. Los comandos han funcionado correctamente (no sin quebraderos de cabeza) 8,5 sobre 10?

Actividad 4: La ultima actividad me ha resultado un autentico suplicio. La primera parte de configuracion del spanning tree y su explicación y justificación ha ido sin ningún problema, pero al llegar a la parte de “demostrar mediante capturas con comandos en los switches” el camino que seguiría el ping me ha tenido 2 días devanandome los sesos como un idiota sin ocurrirseme ningún modo en como justificar la ruta del ping (justificar, que no saber; la ruta que seguiría la tenia clara desde el principio). No tengo nada claro si la solución de mostrar las tablas MAC era lo que se pedía, así que me pondré en el peor de los casos y diré... 5 sobre 10?

Nota final: Tal vez un 7

Por último...

Una vez realizada la tarea, rellena **al final del documento tu autoevaluación justificada por cada actividad y para la tarea en total.**

El envío se realizará a través de la plataforma y el archivo se nombrará siguiendo las siguientes pautas:

Apellido1_Apellido2_Nombre_PAR03_Tarea.pdf

¡IMPORTANTE! Asegúrate que el nombre **no contenga la letra ñ, tildes ni caracteres especiales extraños.**