Universidad de Alcalá

Departamento de Automática

REDES DE COMPUTADORES

Laboratorio

Práctica 4: Funciones generales de la capa de Enlace

Grado en Ingeniería Informática

Curso 2018/19

OBJETIVOS

- Realizar la configuración básica de un Switch CISCO
- Poder implementar 2 simulaciones que expliquen las funciones de capa 2 desarrolladas por un dispositivo Conmutador/Switch
- Evaluar los parámetros de las diversas tramas (PDU capa2) generados por cada dispositivo terminal e intermedio de la red.
- Diferenciar los conceptos de "Dominio de Difusión" y "Dominio de Colisión"

FUNCIONES GENERALES DE LA CAPA 2 OSI

La capa 2 OSI de Enlace de datos proporciona un transito de datos "fiable" a través de un enlace físico de red. De este modo, la capa de enlace de datos se ocupa de los siguientes "Aspectos Claves" dentro de una LAN:

• Direccionamiento Físico de los dispositivos: genera una identificación única a cada host/dispositivo conectado a la red.

• Implementa las Topologías lógicas de una LAN: mediante diversos tipos de dispositivos y protocolos.

• Acceso de Usuarios a una red, Notificación de Errores: emite alertas a los protocolos de las capas OSI superiores cuando ocurre un error de transmisión

• Distribución Ordenada de Tramas: genera una secuencia de tramas para transmitir los "Datos" de un Emisor y en el Receptor se reordenan las tramas recibidas (en desorden, fuera de secuencia)

• Control del Flujo de las comunicaciones dentro de la red: define una moderación de la transmisión de datos de tal manera que el dispositivo receptor no se sobresature con más tráfico que el que puede manejar a un tiempo.

No todas las funciones están implementadas en todos los protocolos: los hay más sofisticados y los hay más básicos. Cada tipo de enlace tiene sus propias necesidades.

DISPOSITIVOS DE LA CAPA 2 OSI

Tarjetas de interfaz de red (NIC)

Una tarjeta de interfaz de red (NIC) es una placa de circuito impreso que proporciona las capacidades de comunicación de red hacia y desde un computador personal. También se le denomina adaptador de LAN y se enchufa en la "placa-base" para así proporcionar un puerto de conexión a una red.

Las NIC están consideradas como dispositivos de la capa 2 OSI porque cada una de ellas tiene un código único, denominado dirección de control de acceso al medio (MAC: media access control, o MAC, establecida por la IEEE). Dicha dirección controla la comunicación de datos para el host en la LAN. Las NIC controlan el acceso del host al medio de la red.

La tarjeta de red actúa como una interfaz física entre el cable de red y la computadora. Existen diferentes tipos de medios sobre los cuales operan las tarjetas de red, pero estas no se conectan directamente al medio ya que necesitan un componente adicional llamado conector, el cual es diferente para cada tipo de medio en el que se usará.

Puente o Bridge

Un puente es un dispositivo de la capa 2 diseñado para dividir a una LAN en dos segmentos, gracias a que constan de 2 puertos de conexión de red. En otras palabras, divide el dominio de colisión inicial, y cada segmento de esta LAN define un dominio de colisión separado.

El propósito de un puente es filtrar el tráfico de una LAN a nivel de la Capa de Enlace de Datos, para que el tráfico local siga siendo local, pero permitiendo que el tráfico que va dirigido hacia ese segmento, pueda ser conectado con otras partes (segmentos) dentro de una LAN.

¿Cómo puede detectar el puente cuál es el tráfico local y cuál no lo es? El puente verifica la dirección local. Cada dispositivo de networking tiene una dirección MAC exclusiva en su NIC, y el puente rastrea cuáles son las direcciones MAC que están ubicadas a cada lado del puente (en cada puerto). Así toma sus decisiones basándose en esta lista de direcciones MAC.

Como los puentes solo se fijan en las direcciones MAC, no se ocupan de los protocolos de la capa 3. En consecuencia, los puentes solo se preocupan de que las tramas pasen o no pasen de un puerto a otro, basándose en sus direcciones MAC destino.

Además, esta función hace que las redes sean más eficientes, al permitir que los datos se transmitan al mismo tiempo a diferentes segmentos de la red LAN, pero sin que colisionen las tramas.

Función de segmentación de una red hecha por un Puente

Cuando el puente recibe una trama en una de sus interfaces, analiza la dirección MAC del emisor y del destino. Si un puente no reconoce al emisor, almacena su dirección en una **Tabla de direcciones MAC** para "**así recordar, en qué lado de la red se encuentra el emisor de la Trama**". De esta manera, el puente puede averiguar si el emisor y el destino se encuentran del mismo lado o en lados opuestos del puente.

En otras palabras, si la MAC del emisor y destino de una Trama se encuentran en…

- … el mismo puerto, el puente ignora/descarta la trama
- … en puertos diferentes del puente, este último hace una copia de la trama, para enviarla hacia el otro puerto donde se encuentra el destino.

Este mecanismo permite un "aprendizaje automático" de todas las MAC conectadas en cada uno de los 2 puertos de un Bridge.

Switch | Conmutador

Un switch, al igual que un puente, es un dispositivo de la capa 2.

De hecho, al switch se le denomina un **puente multipuerto**, así como el hub se denomina **repetidor multipuerto**. A primera vista, un switch se parece a menudo un hub. Tanto los hubs como los switches tienen varios puertos de conexión, dado que una de las funciones de ambos es la concentración de conectividad (permitir que varios dispositivos se conecten a un punto de la red).

La diferencia básica entre un hub y un switch está dada por lo que sucede dentro del dispositivo. Un switch toma decisiones basándose en las direcciones MAC y los hubs no toman ninguna decisión.

Como los switches son capaces de tomar decisiones, hacen que una LAN sea mucho más eficiente. Los switches hacen esta tarea "conmutando" las tramas hacia solamente el puerto al cual está conectado el Host destino correspondiente.

Un hub en cambio, envía datos a través de todos sus puertos de modo que todos los hosts deben ver y procesar (aceptar o rechazar) la trama enviada.

El propósito principal del switch es concentrar la conectividad, haciendo que la transmisión de datos sea más eficiente. Piensa en el switch como un dispositivo de red que puede combinar la conectividad de un hub con la regulación de tráfico de un puente en cada uno de sus puertos.

MAC ETHERNET (IEEE 802.3)

Ethernet es una Topología de Difusión de Medio Compartido (red lógica en bus) que puede transmitir datos a 10 Mbps. Esto significa que todos los dispositivos ven las tramas transmitidas a través del Medio compartido, pero solo el host Destino las procesa.

Utiliza un mecanismo de control de acceso al medio MAC denominado Acceso Múltiple con detección de portadora y detección de colisiones (CSMA-CD: Carrier-Sense Multiple Access with Collision Detection), el cual regula el tráfico de la red, permitiendo la transmisión en la red sólo cuando esta esté despejada y no haya otro equipo transmitiendo. CSMA/CD permite que todos los hosts de una LAN tengan acceso al medio físico común de red en condiciones similares.

Temporizacion Ethernet

Ethernet se diseñó para operar en una estructura de bus, lo cual significa que cada estación siempre escucha todos los mensajes casi al mismo tiempo, utilizando el método CSMA/CD.

Las normas Ethernet establecen que cualquier estación en una red que quiere transmitir un mensaje, primero escucha para asegurarse que no hay ninguna otra estación transmitiendo en ese momento. Si el cable esta libre, la estación comienza su transmisión de inmediato. Pero las señales eléctricas necesitan una cantidad de tiempo pequeña (llamada retardo de propagación) para viajar a través del cable, y cada repetidor que encuentre la trama introduce una pequeña latencia en el envío de la trama de un puerto al siguiente, lo que origina que mas de una estación comience a transmitir al mismo tiempo, provocando una **Colisión**.

Manipulación de errores de la tecnología Ethernet

La condición de error más común en Ethernet es la colisión. La colisión es el mecanismo para resolver el acceso a una LAN. Las colisiones solo son posibles en los segmentos semiduplex.

Las colisiones normalmente tienen lugar cuando dos o mas estaciones Ethernet transmiten simultáneamente dentro de un dominio de colisión. Al resultado de las colisiones (ya sean tramas parciales o totalmente corruptas, que tienen menos de 64 octetos y un FCS no valido) se les llaman a menudo **fragmentos de una colisión** o **runts**.

Los principales tipos de errores con tramas Ethernet que se pueden capturar mediante una sesión de análisis de protocolo son:

a) Colisión local b) Colisión remota c) Colisión atrasada

INTRODUCCION AL IOS DE UN DISPOSITIVO DE RED

El sistema operativo Internetwork (IOS) de Cisco

Al igual que un computador (PC), un router o switch no pueden funcionar sin un sistema operativo. El sistema operativo Internetwork (IOS) de Cisco es el software del sistema en los dispositivos Cisco, independientemente del tamaño o tipo de dispositivo. Se usa en routers, switches LAN, pequeños puntos de acceso inalámbricos, grandes routers con decenas de interfaces y muchos otros dispositivos.

Las operaciones realizadas por el IOS varían de acuerdo con los diferentes dispositivos de red, según el propósito y el conjunto de características del dispositivo. Entre los servicios de red que el Cisco IOS provee a sus dispositivos están: Seguridad, direccionamiento, manejo interfaces y Calidad de servicios.

El archivo del IOS es de varios megabytes y se encuentra en un área de memoria semipermanente llamada flash. La memoria flash provee almacenamiento no volátil, que hace que los contenidos de la memoria no se pierdan cuando el dispositivo se apague, pero también se puedan modificarse o sobrescribirse cuando sea necesario.

Modos de Conexión/Acceso para la administración de los dispositivos

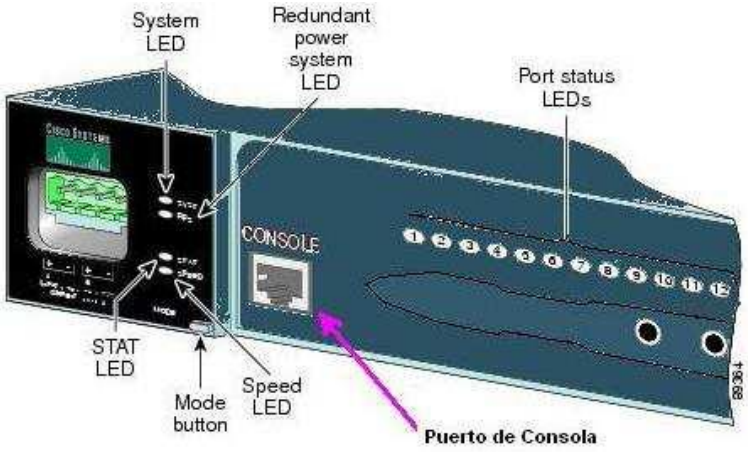
Para establecer la conexión física entre PC del administrador (que ejecuta el Emulador de terminal) y el dispositivo, existen varias formas de acceder al entorno de la CLI. Los métodos más comunes son:

a) Consola b) Telnet o SSH

El método más común es conectar un equipo al puerto de Consola del dispositivo mediante el método de Consola. Este utiliza un Cable de Consola, conectando la interfaz de un puerto serial EIA/TIA 232 disponible en el PC, con un conector DB-9 en un extremo y un conector RJ-45 en el otro, que es el que se conecta a un puerto de Consola (ver figuras , el puerto CONSOLE).

El puerto de consola es un puerto de administración importante, porque provee acceso al dispositivo fuera de banda, lo que significa que se puede tener acceso al dispositivo cuando aún no se han iniciado sus servicios de red o han fallado incluso.

Vista trasera de un Switch de la serie Cisco Catalyst 2950, que muestra los diversos puertos de conexión Fast Ethernet.



Vista frontal de un Switch de la serie Cisco Catalyst 2950, que muestra los indicadores de funcionamiento, el puerto de Consola (Console) y el puerto Auxiliar (AUX)

Telnet y SSH

Otro de los métodos que sirve para acceder en forma remota a la sesión CLI es hacer telnet al dispositivo. A diferencia de la conexión de consola, las sesiones de Telnet requieren servicios de networking activos en el dispositivo de red. Este debe tener configurada por lo menos una interfaz activa con una dirección de Capa 3, por ej.: una dirección IPv4. Los dispositivos Cisco IOS incluyen un proceso de servidor Telnet que se activa cuando se inicia el dispositivo. El IOS también contiene un cliente Telnet.

EMULADOR DE TERMINAL Y LA INTERFAZ DE LÍNEA DE COMANDOS (CLI)

Debido a que la mayoría de dispositivos de red administrables con IOS no tienen sus propias pantallas ni dispositivos de entrada (un teclado o ratón), el acceso para la configuración y administración de los mismos se realiza mediante una conexión lógica entre el dispositivo y un PC. Para comunicarse mediante la línea serie se utilizan programas de emulación de terminal.

Un emulador de terminal es un software que permite a un computador comunicarse a través de una línea serie a las funciones de otro dispositivo. Permite a una persona utilizar el teclado y pantalla de su PC para indicar operaciones que son ejecutadas en el otro dispositivo.

Uno de los emuladores de terminal más utilizados bajo Windows es *HyperTerminal*, que ya viene incluido en la mayoría de de las versiones de Windows. Para el mundo Unix/Linux un emulador de terminal típico es el

minicom (aunque existen otros). En cualquier caso, hay que configurar la línea serie de acuerdo a lo especificado por el dispositivo terminal. Los parámetros para una línea serie típica son los siguientes:

Bits por segundo: 9600 bps

Bits de datos: 8

Paridad: Ninguna

Bits de parada: 1

Control de flujo: Ninguno

Si se realizan correctamente todas las configuraciones y conexiones de cables, se podrá acceder al dispositivo al presionar la tecla Intro del teclado, desde la ventana del software emulador de terminal, mostrándose la CLI.

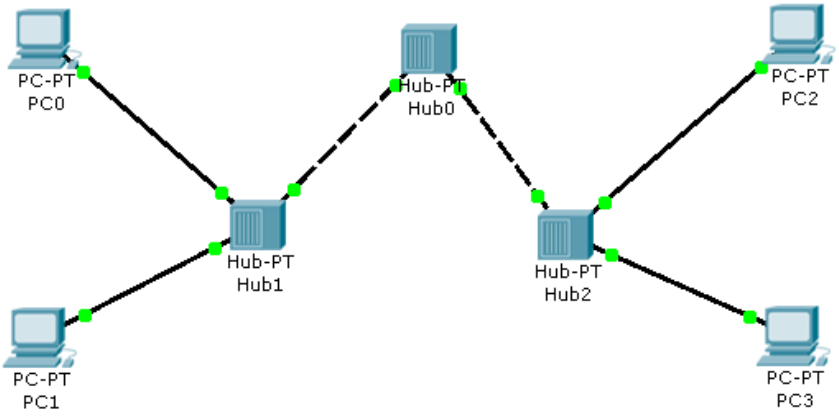
La Interfaz de línea de comandos (CLI) permite acceder a los servicios que proporciona el IOS, por medio de una serie de comandos, que invocan las diferentes funciones de administración del dispositivo. Las funciones accesibles a través de la CLI varían según la versión de IOS y el tipo de dispositivo.

PRÁCTICA

PARTE I-A: Diseñando una Red LAN Ethernet en topología Estrella Extendida

- Acceder a la aplicación Packet Tracer.
- Personalizar el entorno de trabajo del Modo Tiempo Real (RealTime) del simulador, ingresando en el menú principal (Opciones/Preferencias) y en la pestaña Interfaz, marcar la opción "Always Show Port Labels". Cerrar esta ventana.
- Crear la Topología de Red Ethernet mostrada a continuación. Esta utilizará dispositivos Hub-PT (Hubs/Concentradores de Capa Física) y PC-PT (cada Host es un equipo terminal de datos DTE), además de cables planos o cruzados (de acuerdo a los dispositivos a conectar).

IP DE RED: 195.5.0.0, Máscara: 255.255.255.0



- Asignar a los PC's direcciones IP dentro de su rango de direccionamiento y rellenar la siguiente tabla de direccionamiento MAC e IP para cada equipo DTE (cada uno de los host).

  En todos los casos aún no se asignará la IP de Puerta de enlace (Default Gateway).

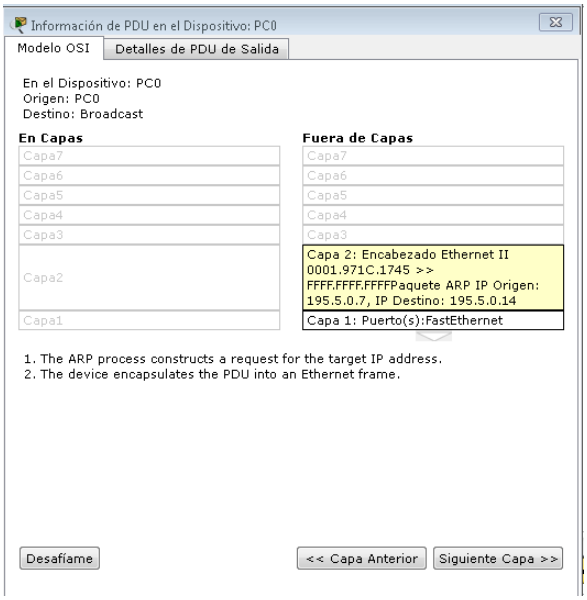
DTE	MAC(a)	IP (a asignar)
PC0		
PC1		
PC2		
PC3		

- Cambiar al modo de Simulación. Ahora habrá que hacer las pruebas de comunicación con el comando ping desde PC0, dirigido a la IP asignada a PC1.
- Hacer clic sobre PC0, pinchar en la pestaña Escritorio y seleccionar la opción "Símbolo del Sistema". Se mostrará una ventana con el entorno MSDOS.
- Teclear el comando arp –a, ¿qué información se visualiza?
- Escribir el comando ping dirigido a la IP asignada a PC1 y dar a la tecla Enter, se observará lo siguiente:

  Cerca de PC0 surgen 2 cuadros (simulando 2 tramas (con apariencia de "sobres")), junto a 2 eventos en la ventana Event List.

  La primera trama lista a transmitir utiliza el protocolo ARP y la segunda ICMP.

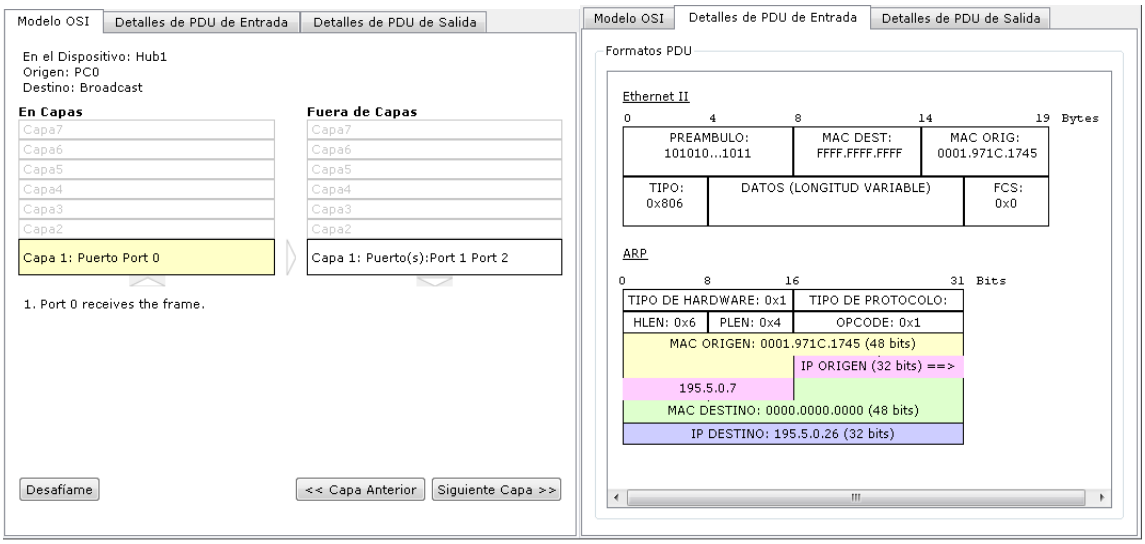
- Desplazar el ratón sobre cada trama y dar clic sobre la que diga Tipo ARP (debido a que será la primera que transmitirá PC0)
- Se muestra la ventana "Información de PDU en el Dispositivo: PC0", (Observar la figura de abajo) con la composición de los protocolos y los datos para cada capa OSI de la PDU (Unidad de Datos de Protocolo).



  - *Esta es una trama de salida (Fuera de Capas) que transmitirá PC0 por el medio físico.*
  - *Debido a que PC0 conoce su propia MAC e IP, pero no sabe la MAC de PC1, utilizará el protocolo ARP con el fin de determinar la MAC (Capa 2) de PC1.*
  - *Esta trama contiene una MAC destino de difusión (todos los 48 bits a 1) y su propia MAC como origen. Además, encapsulados en su campo de datos, lleva ambas direcciones IP (de capa 3) de Origen-Destino (que si las conoce).*

- Selecciona la ficha superior **Detalles de PDU de Salida** y estudia su contenido.
- Cierra la ventana "Información de PDU en el Dispositivo: PC0" y vuelve a la ventana de comandos de PC0, verás que el comando ping aún no se ha ejecutado, porque requiere que se presione el botón (Auto Captura/Reproducir) de la ventana Lista Eventos (Event List)
- Presiona el botón (Auto Captura/Reproducir) y presiónalo de nuevo antes de que la trama ARP llegue al Hub1. Ahora analiza lo siguiente:
  - En la lista de eventos se ha creado un 3er evento [**desde (Último dispositivo) PC0 hasta (En dispositivo) Hub1**]
  - El tipo de esta trama recibida sigue siendo ARP (porque un Hub no puede alterar datos de una trama recibida, solo los retransmite)

- Da clic en esta nueva trama ARP (recibida por Hub1). Observa que un Hub sólo cambia la PDU de la trama a nivel de capa física (PDU: Bits). Indica que recibió trama por Puerto 0 y está listo para envíar "copias idénticas" por sus puertos restantes. Dentro de la tecnología MAC Ethernet, a este proceso se le llama Difusión/Broadcast.
  - *Nota: Esta descripción se puede obtener al dar clic sobre cada capa (sea de entrada o de salida) dentro de la ventana de descripción de las PDU actual (la capa se marca en amarillo, describiendo debajo el significado de la PDU seleccionada)*



Construcción y detalles de trama enviadas durante Modo Simulador de Packet Tracer

- Cerrar la ventana de PDU's y cuidadosamente repetir sólamente los 2 pasos anteriores. Verás que el Hub reenvía "una copia" de la capa recibida hacia todos sus puertos, ¡excepto por el que lo recibió!

- Al estudiar cada trama, notarás que la NIC de PC1 "comprende hasta la PDU Capa2 (Trama)", en cambio, el Hub0, ve solamente Bits (PDU capa 1), porque solo le interesa enviar bits recibidos hacia su otro puerto

- Repetir los pasos necesarios para seguir la pista a cada trama enviada.

IMPORTANTE: Observar que PC1 es el único que prepara una trama de respuesta ARP a PC0. Los demás PC's descartan la trama recibida.

- Finalmente, cuando veas que en la ventana de comandos se han enviado los cuatro paquetes y permanece a la espera, teclea de nuevo arp –a, ¿qué se ve ahora?.

- Extraer las conclusiones pertinentes.

PARTE I-B: Identificando Dominios de Difusión y Colisión

- Guarda el archivo actual "Guardar como" con el nombre P4_1A y crea una copia con el nuevo nombre P4_1B.
- Con esta nueva simulación, conectar un nuevo PC (PC4) en Hub1 y otro PC (PC5) en Hub2. Asignar IP's de host dentro del rango de la red que estás utilizando.
- Cambiar a modo Simulación. Realizar las acciones necesarias para ejecutar el comando ping desde 2 PC diferentes entre sí: de PC0 a PC1, así como ping de PC2 a PC4. PERO NO PRESIONAR AÚN el botón Play. Observar nuevamente la pareja de tramas (ARP y ICMP) listas en cada DTE origen de la transmisión (PC0 y PC2).
- Desde la Ventana de Eventos, presionar el botón Play y observar como las tramas ARP de ambos DTE "viajan/saltan de equipo a equipo", "como los hubs reproducen cada trama por sus puertos" y cuando ocurre una colisión.

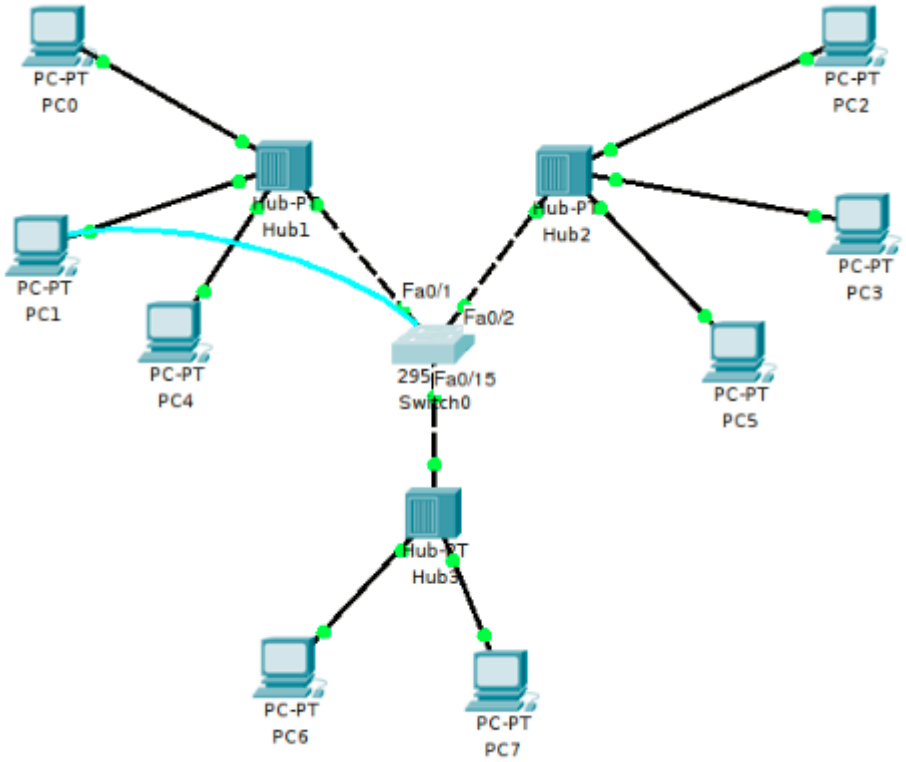
  Prestar mucha atención a la manera como los PC's reinician sus transmisiones y responder estas preguntas:
  - Después de una colisión, ¿Los DTE reintentan envío de tramas al mismo tiempo o en momentos diferentes?
  - Luego de unos 30 seg. (aprox.), ¿logran PC0 y PC2 determinar la MAC de sus DTE destinos respectivos?

- ¿Se cumplen las normas del método CSMA/CD?, si o no ¿Por qué?
- ¿Cuántos Dominios de Difusión/Broadcast y Dominios de Colisión existen en esta topología de red que has elaborado?

PARTE II-A: Configuración básica de un Dispositivo de Red. Estableciendo una sesión de consola con un Switch

- Guardar la configuración del apartado anterior (P4_1B),, realizar ahora una copia de la misma con el nombre Pract_3.
- Eliminar el Hub principal (Hub0) y luego agregar un switch 2950T-24 a la topología.
- Incluir otra pareja de 2 PC's (PC6 y PC7) conectados a un nuevo Hub (Hub3) y este a su vez conectarlo al puerto FastEthernet 0/15 del Switch0 central por medio de un cable cruzado. Asignar el direccionamiento IP respectivo a estos 2 nuevos.
- Localizar en la topología a PC1, desde el cual se iniciará una sesión directa de consola con el Switch0 de la red a continuación.

Seleccionar un cable para conexión de Consola (Console) y dar clic sobre el PC1 seleccionado para el enlace y marcar en su interfaz serial (RS-232). Luego dar clic en Switch0 y seleccionar su interfaz de Consola.



- Ahora ingresar al IOS del Switch0 por medio del software del Emulador de Terminal del PC1. Para ello da clic sobre PC1 que usará para la administración del switch, localizar la pestaña Escritorio/Desktop y luego localizar el botón Terminal.
- Observar que se simula la ventana de configuración de parámetros para establecer la "Configuración de la terminal". Confirmar en Aceptar/Ok.
- De esta manera, se ingresará a la CLI (Command Line Interface) para la administración del ISO del Switch0 por medio de una ventana de comandos.

- Presionar Intro para ingresar al Modo de Ejecución del Usuario (o Modo EXEC del usuario) del IOS del Switch0. Sabrás que se encuentra en el mismo, gracias al cursor presentado: Switch>
- Este modo EXEC usuario permite ejecutar sólo una cantidad limitada de comandos de monitoreo básicos, de visualización solamente. No permite la ejecución de ningún comando que pueda cambiar la configuración del dispositivo.

PARTE II-B: Identificando Dominios de Difusión y Colisión

- Con este escenario, Fig. 2, entrar en modo simulación y ejecutar el comando ping entre los terminales PC0-PC4 y simultáneamente entre PC2-PC7. Observar cuidadosamente los paquetes intercambiados en los equipos.

  ¿Han desaparecido las colisiones?

  ¿Cuántos Dominios de Difusión/Broadcast y Dominios de Colisión existen en esta topología de red?
- Pulsa el icono "Lupa" y acercarlo al conmutador. Hacer que muestre la tabla de direcciones MAC.
- Repetir varias veces el ping anterior.

  ¿Qué diferencias se observan?

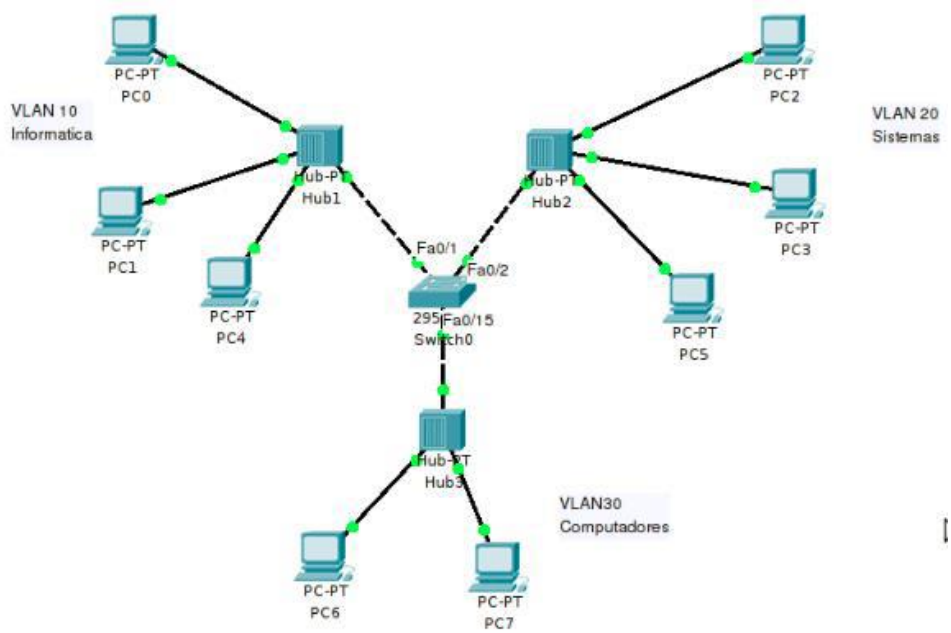
  ¿Qué contiene la tabla de direcciones MAC? ¿Ha ido cambiando conforme ejecutábamos los comandos ping anteriores?

  Buscar el comando equivalente para mostrar la tabla de direcciones MAC desde el CLI.

PARTE III: Configuración de VLANS

- Guardar la configuración del apartado anterior (P4_2) y realizar una copia de la misma con el nombre P4_3.

Vamos a configurar ahora las siguientes VLAN en nuestro esquema:



- Antes de nada, Revisa el estado de las tablas arp de los equipos, (utilizando la lupa y posicionándola encima de cada equipo). Haz lo mismo con el switch y revisa la MAC table.

  Fíjate también en Port status y veras que todos los puertos están dentro de la VLAN 1 (default).

Envía un ping desde pc0 a pc1 y revisa de nuevo las tablas.

- Haz doble click en el switch y desde el menú de config selecciona VLAN Database.

- Añade la VLAN 10 de nombre Informática, la VLAN 20 Sistemas y la VLAN 30 Computadores.

Fíjate que lo que estamos haciendo de una manera gráfica podríamos hacerlo desde CLI introduciendo los comandos. Presta atención a los comandos equivalentes en: Equivalent IOS Command.+

- En la pestaña de las interfaces FastEthernet 0/1, 0/2 y 0/15 añade dichos puertos a las VLAN 10, 20 y 30 respectivamente.

Desde el modo **Simulación:**

Envía un paquete desde el PC0 a PC1 y desde PC6 a PC7.

Pulsa Capture/Forward (Mejor que Auto Capture/Play) para ver paso a paso que es lo que sucede. Fíjate muy bien en como son los paquetes que se envían, quienes los reciben y quienes los descartan. Revisa de nuevo la MAC Table. Haz cuantas pruebas consideres oportunas.

Responde a lo siguiente:

¿Cuántos dominios de colisión hay? ¿Cuántos dominios de difusión hay?

Explícalo y saca **conclusiones.**

- Replica ahora la configuración anterior, colgando de un nuevo conmutador otros tres grupos de terminales, cada uno de ellos en cada una de las tres redes virtuales (VLAN 10 Informática, la VLAN 20 Sistemas y la VLAN 30 Computadores).

- Une ambos conmutadores mediante un enlace troncal de manera que las redes virtuales colgadas de cada conmutador se vean entre sí.

- Comprueba la conectividad entre todas las redes virtuales.

  ¿Cuántos dominios de colisión hay ahora? ¿Cuántos de difusión?

- Entrando en el modo simulación, observa las tramas que se circulan por el enlace troncal.

  ¿Qué formato tienen esas tramas? ¿Qué información transportan?