



INSTITUTO TECNOLÓGICO SUPERIOR DE CHICONTEPEC

“Por la Excelencia Educativa”

INGENIERÍA EN SISTEMAS COMPUTACIONALES

MATERIA:

Diseño De Redes de Campus Y WAN

Nombre Del Tema:

Estándar IEEE 802.3.

Nombre De La Actividad:

Reporte.

Grupo: ISC-8S

Alumno:

Jorge Javier De La Cruz Hernández

Docente:

Ing. Francisco Javier Hernández Hernández

Chicontepec de Tejeda, Veracruz marzo 2023:

Diseño De Redes Campus Y WAN G2-23

1.- Introducción.....	3
2.- Fundamento teórico.....	4
¿Qué es Ethernet (¿IEEE 802?3)?.....	4
Capa 1 y capa 2.....	5
Control de enlace lógico: conexión con las capas superiores.....	6
Diferencias entre transmisiones Unicast, Multicast y Broadcast.....	7
Capa física de Ethernet.....	8
Función y dese.....	9
Empeño Switch / Hub	9
Qué es un Switch	10
En qué consiste el protocolo ARP	10
La dirección MAC	11
Una red de área local (LAN).....	12
4.- Metodología.....	13
1.- Configuración de una red local a través de VLAN.....	13
2.-Ejemplo de práctica de ARP.....	21
Practica por medio del CMD ARP.....	23
5.- Resultados	24
Resultado de la red local a través de VLAN.....	24
Resultado de Practica de ARP	25
Resultado del ARP por medio del CMD	27
6.- Conclusiones.....	28
Bibliografía.....	29

1.- Introducción

En este reporte se verá reflejado una práctica donde nosotros configuraremos una red local en ello interactuara la red local VLAN ya que va de la mano con el reporte anterior donde nosotros creamos una red de acuerdo con los datos que se recopiló, el filtrado MAC que como sabemos es un método de seguridad al momento de tener un red de internet en base a ello también se verá reflejado como poder utilizar el ARP que es una de las actividades que se han programado en este reporte de igual manera en ello viene una investigación de todo lo relacionado con la unidad que se vio en clase todo acerca de la seguridad de una red de internet ya que como sabemos tiene que llevar ciertos parámetros y configuraciones para que la red este segura.

2.- Fundamento teórico.

¿Qué es Ethernet (¿IEEE 802.3)?

Ethernet es una tecnología para redes de datos por cable que vincula software y/o hardware entre sí. Esto se realiza a través de cables de redes LAN, de ahí que Ethernet sea concebido habitualmente como una tecnología LAN. Así, Ethernet permite el intercambio de datos entre terminales como, por ejemplo, ordenadores, impresoras, servidores, distribuidores, etc. Conectados en una red local, estos dispositivos establecen conexiones mediante el protocolo Ethernet y pueden intercambiar paquetes de datos entre sí. El protocolo actual y más extendido para ello es IEEE 802.3.

Ethernet fue desarrollado a principios de los 1970, época en la que solo se utilizaba como sistema interno de red en la empresa Xerox, y no fue hasta principios de los ochenta que Ethernet se convirtió en un producto estandarizado. Con todo, aún habría que esperar hasta mediados de la década para que empezara a utilizarse más ampliamente. Fue cuando los fabricantes comenzaron a trabajar con Ethernet y con productos relacionados. Así, dicha tecnología contribuyó (Digital Guide, s.f.) de manera significativa a que los ordenadores personales revolucionaran el mundo laboral. El estándar IEEE 802.3 tan popular actualmente se utiliza, por ejemplo, en oficinas, viviendas particulares, contenedores y portadores (carrier).

Mientras que la primera versión de esta tecnología solo tenía una velocidad de 3 Mbit/s, los protocolos Ethernet actuales permiten alcanzar velocidades de hasta 1 000 megabits por segundo. Por otro lado, los estándares Ethernet antiguos se restringían a un solo edificio, mientras que hoy en día pueden alcanzar hasta los 10 km gracias a la utilización de la fibra de vidrio.

Capa 1 y capa 2

Ethernet opera a través de dos capas del modelo OSI. El modelo ofrece una referencia sobre con qué puede relacionarse Ethernet, pero en realidad se implementa sólo en la mitad inferior de la capa de Enlace de datos, que se conoce como subcapa Control de acceso al medio (Media Access Control, MAC), y la capa física.

Ethernet en la Capa 1 implica señales, streams de bits que se transportan en los medios, componentes físicos que transmiten las señales a los medios y distintas topologías.

La Capa 1 de Ethernet tiene un papel clave en la comunicación que se produce entre los dispositivos, pero cada una de estas funciones tiene limitaciones.

Tal como lo muestra la figura, Ethernet en la Capa 2 se ocupa de estas limitaciones. Las subcapas de enlace de datos contribuyen significativamente a la compatibilidad de tecnología y la comunicación con la computadora.

La subcapa MAC se ocupa de los componentes físicos que se utilizarán para comunicar la información y prepara los datos para transmitirlos a través de los medios.

La subcapa Control de enlace lógico (Logical Link Control, LLC) sigue siendo relativamente independiente del equipo físico que se utilizará para el proceso de comunicación. (Redes de computadoras, s.f.)

Control de enlace lógico: conexión con las capas superiores

Ethernet separa las funciones de la capa de Enlace de datos en dos subcapas diferenciadas: la subcapa Control de enlace lógico (LLC) y la subcapa Control de acceso al medio (MAC). Las funciones descritas en el modelo OSI para la capa de Enlace de datos se asignan a las subcapas LLC y MAC. La utilización de dichas subcapas contribuye notablemente a la compatibilidad entre diversos dispositivos finales.

Para Ethernet, el estándar IEEE 802.2 describe las funciones de la subcapa LLC y el estándar 802.3 describe las funciones de la subcapa MAC y de la capa física. El Control de enlace lógico se encarga de la comunicación entre las capas superiores y el software de red, y las capas inferiores, que generalmente es el hardware. La subcapa LLC toma los datos del protocolo de la red, que generalmente son un paquete IPv4, y agrega información de control para ayudar a entregar el paquete al nodo de destino. La Capa 2 establece la comunicación con las capas superiores a través del LLC.

El LLC se implementa en el software y su implementación depende del equipo físico. En una computadora, el LLC puede considerarse como el controlador de la Tarjeta de interfaz de red (NIC). El controlador de la NIC (Tarjeta de interfaz de red) es un programa que interactúa directamente con el hardware en la NIC para pasar los datos entre los medios y la subcapa de Control de Acceso al medio. (Redes de computadoras, s.f.)

Diferencias entre transmisiones Unicast, Multicast y Broadcast.

En cualquier Red local (Lan, ethernet) que funciona bajo IPv4 los métodos de transmisión de datos están diferenciados en 3 tipos, Unicast, Multicast y Broadcast.

Unicast:

Según este método de transmisión, una trama (frame) es enviada desde una única interfaz de salida a una única interfaz de destino, es lo que denominamos transmisión uno-a-uno (one to one).

Es el de mayor uso en internet, a pesar de que gestionar las conexiones con este método tiene un gran impacto negativo en el ancho de banda y en los recursos de equipo, por eso algunas aplicaciones requieren, en su mayoría streaming de medios (audio, video), de una red separada y dedicada a ello.

Multicast: Este método de transmisión se caracteriza por ser el que envía de una interfaz de salida un grupo de interfaces de destino simultáneamente, es similar al broadcast sólo que en multicast se envía a un grupo específico y el broadcast envía a todos los nodos de red.

Gracias a este método de transmisión se ahorra una gran cantidad de ancho de banda al dirigir la información sólo al grupo seleccionado y la mayor parte de los datos son enviados en una sola transmisión.

Broadcast:

La transmisión broadcast es aquella que difunde la información de forma simultánea a todos los nodos de red. Es el método de comunicación más generalizado y el más intensivo ya que requiere de una gran cantidad de mensajes, dependiendo del número de hosts en la red. (Tech Club, s.f.)

Capa física de Ethernet

La capa física de Ethernet es el componente de capa física del estándar Ethernet.

La capa física de Ethernet evolucionó sobre un considerable período de tiempo y abarca completamente algunas interfaces de medios físicos y varias magnitudes de velocidad.

La velocidad se extiende desde 1 Mbit/s a 40 Gbit/s (velocidades más altas están en desarrollo) mientras que el medio físico puede extenderse desde el cable coaxial voluminoso, al par trenzado, hasta la fibra óptica. En general, el software del stack de protocolo de la red trabajará similarmente en todos los tipos que se describirán más adelante.

Las secciones siguientes proporcionan un breve resumen de todos los tipos de medios oficiales de Ethernet (los números de sección del estándar IEEE 802.3-2008 están entre paréntesis).

Adicionalmente de estos estándares oficiales, muchos vendedores han implementado tipos de medios propietarios por varias razones - a menudo para soportar distancias más largas sobre el cableado de fibra óptica.

Muchos adaptadores de Ethernet y puertos de switches soportan múltiples velocidades, usando auto negociación para ajustar la velocidad y la modalidad duplex para los mejores valores soportados por ambos dispositivos conectados.

Si la auto-negociación falla, un dispositivo de múltiple velocidad detectará la velocidad usada por su socio, pero asumirá semiduplex. Un puerto Ethernet 10/100 soporta 10Base-T y 100Base-TX. Un puerto Ethernet 10/100/1000 soporta 10Base-T, 100Base-TX, y 1000Base-T. (Wikipedia, s.f.)

Función y dese

Empeño Switch / Hub

Qué es un hub

Lo primero que tenemos que tener claro es que un hub es mucho más simple que un switch, y actualmente ya no se utilizan debido al rendimiento que proporcionan y a las pocas posibilidades de configuración que disponemos. Cuando usamos un hub y un equipo envía una trama de datos a la red, esta trama pasa por el hub, y el propio dispositivo se encarga de enviarlo por todas las bocas de red excepto por donde la ha recibido. Es decir, el hub no sabe a qué equipo va destinado y los envía a todos.

El hub nació hace décadas con el objetivo de proporcionar una forma de interconexión a diferentes equipos que utilizan la tecnología Ethernet, de hecho, la velocidad máxima que puede tener un switch hoy en día es de 10/100Mbps, no existen hubs que tengan velocidades Gigabit ni tampoco superiores como Multigigabit. Un hub se comporta como un medio de enlaces compartidos, por tanto, se pone en marcha el protocolo CSMA/CD para detectar posibles colisiones y reenviar las tramas nuevamente para que lleguen a su destino.

Debido a su funcionamiento, consumen mucho ancho de banda. Van a necesitar que los bits que se envían vayan al resto de aparatos conectados y no solo al dispositivo destinatario, como puede ser un ordenador. Esa es una desventaja clara y hay que tenerla en cuenta al usar estos aparatos. De hecho, al estar limitados a Fast Ethernet va a hacer que el problema de la velocidad sea uno de los más evidentes.

Actualmente los hubs ya no se venden y ya no se utilizan, a favor del switch que es la evolución del hub con mejoras muy importantes. Es lógico si tenemos en cuenta las limitaciones de este tipo de aparatos y la pequeña diferencia en precio respecto a un switch, que sí que permite obtener mayor velocidad y no tener ciertos problemas.

Qué es un Switch

Cuando conectamos un equipo a un switch este internamente tiene una CAM (Content Addressable Memory) donde almacena información importante de la red, como las direcciones MAC que hay conectadas en los diferentes puertos físicos y si tenemos alguna VLAN asociada a un determinado puerto. De esta forma, cuando al switch le llega un paquete de datos de algún equipo, lee el encabezado de datos y sabe a qué equipo va y lo desvía por el puerto correcto, mirando previamente la tabla CAM construida. Es decir, la diferencia es que el hub envía todos los datos que recibe por todos los puertos y el switch lo envía solo al puerto del equipo correcto.

Un detalle importante es que el switch utiliza una arquitectura store-and-forward, es decir, almacena la trama de datos en un pequeño buffer, para posteriormente reenviarla a su destinatario correcto. (Espinosa, Redes Zone, 2022)

En qué consiste el protocolo ARP

ARP son las siglas de Address Resolution Protocol. En español lo podemos traducir como Protocolo de resolución de direcciones. Es un protocolo de comunicaciones muy importante, ya que se encarga de vincular una dirección MAC o dirección física, con una dirección IP o dirección lógica. Este protocolo se desarrolló en la década de 1980 y hoy en día sigue siendo fundamental para el buen funcionamiento de las redes.

La dirección IP se trata de un número que se le asigna y hace referencia a un equipo en una red. Tiene como fin el facilitar que estos se distingan dentro de la misma. Puede ser pública o privada. En cuanto a la primera, es la que nos facilita nuestro proveedor de internet (ISP), y que nos identifica en Internet. Por otro lado, la privada es la que se establece en los dispositivos dentro de nuestra red doméstica.

En cuanto a la dirección MAC, es el número que identifica un componente de un equipo. En este caso, la tarjeta de red. Pueden ser utilizadas para permitir o denegar el acceso a internet de un equipo.

Se encarga de permitir que un dispositivo conectado a una red pueda obtener una ruta MAC de otro equipo que está conectado a esa misma red, es decir, se encarga de «localizar» donde están los demás dispositivos cableados o inalámbricos en la red, preguntando por la dirección MAC de cada uno de ellos enviando un paquete a la dirección de broadcast que es FF: FF: FF: FF: FF: FF. Permite transmitir datos a través de una trama, ya que este protocolo se encuentra a nivel de capa de enlace. Es importante ya que la longitud de las direcciones IP y MAC no son iguales. La primera tiene una longitud de 32 bits y la segunda de 48 bits. (Jiménez, 2022)

La dirección MAC

Es un identificador único que los fabricantes asignan a una tarjeta o dispositivo de red. También es conocida como dirección física y está formada por 48 bits, representados por dígitos hexadecimales. Cada dirección MAC es única a nivel mundial y, en teoría, son fijas para cada dispositivo.

Cada dirección MAC incluye seis parejas de números. Los primeros tres pares sirven para identificar al fabricante (existen buscadores como este por si tenéis curiosidad) y los tres siguientes al modelo concreto. Es importante tener en cuenta que un equipo puede contar con hardware variado para conectarse a las redes; de esta forma, es común tener una dirección MAC para Ethernet, otra para WiFi y otra para Bluetooth.

Los usuarios domésticos rara vez tienen que hacer uso de la dirección MAC, pero si resultan muy útiles para los administradores de sistemas que tienen que gobernar redes con cientos o miles de dispositivos conectados. Las direcciones MAC se pueden cambiar y no es especialmente complicado. De hecho, en ocasiones se suele recomendar el filtrado de MAC dentro de una estrategia de protección de nuestra conexión que incluya otras acciones como ocultar la SSID, cambiar la contraseña a WAP2 o desactivar el acceso remoto al router. (Cabacas, 2019)

Una red de área local (LAN)

Es un grupo de computadoras y dispositivos periféricos que comparten una línea de comunicaciones común o un enlace inalámbrico a un servidor dentro de un área geográfica específica. Una red de área local puede servir a tan solo dos o tres usuarios en una oficina en casa o miles de usuarios en la oficina central de una corporación. Los propietarios de viviendas y los administradores de tecnología de la información (TI) configuran una LAN para que los nodos de la red puedan comunicarse y compartir recursos como impresoras o almacenamiento en red.

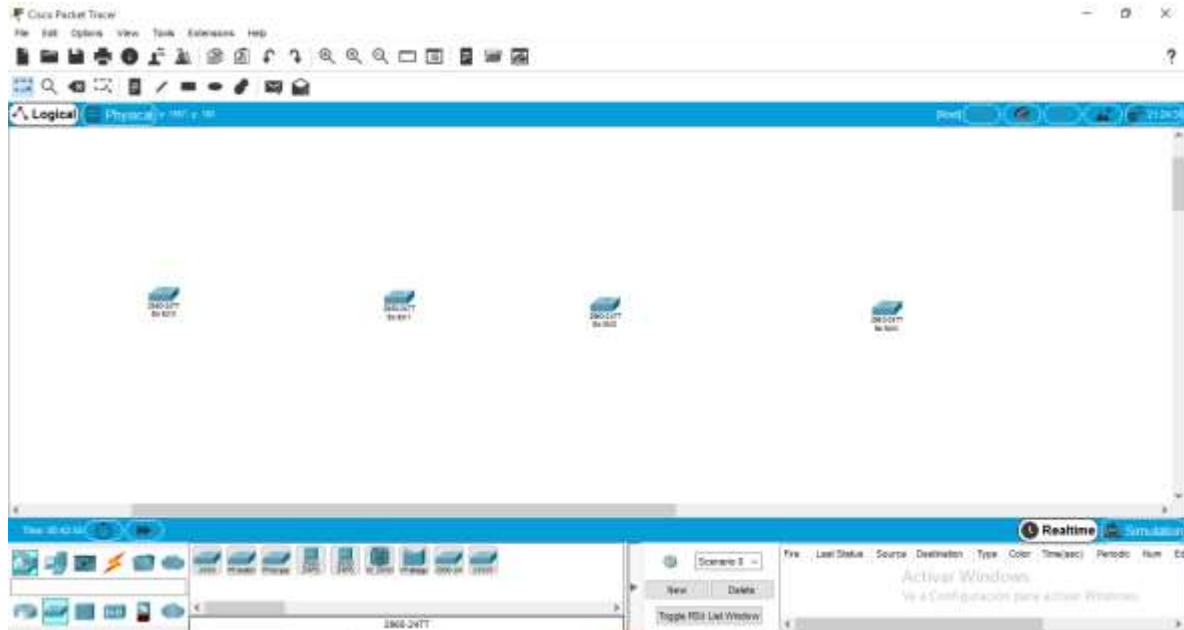
La red LAN requiere cables Ethernet y conmutadores de Capa 2 junto con dispositivos que se puedan conectar y comunicarse mediante Ethernet. Las LAN más grandes a menudo incluyen conmutadores o enrutadores de capa 3 para agilizar los flujos de tráfico.

Una LAN permite a los usuarios conectarse a servidores internos, sitios web y otras LAN que pertenecen a la misma red de área amplia (WAN). Ethernet y Wi-Fi son las dos formas principales de habilitar las conexiones LAN. Ethernet es una especificación del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) que permite que las computadoras se comuniquen entre sí. Wi-Fi utiliza ondas de radio en el espectro de 2,4 gigahercios (GHz) y 5 GHz para conectar computadoras a la LAN. (Diana Hwang, s.f.)

4.- Metodología

1.- Configuración de una red local a través de VLAN.

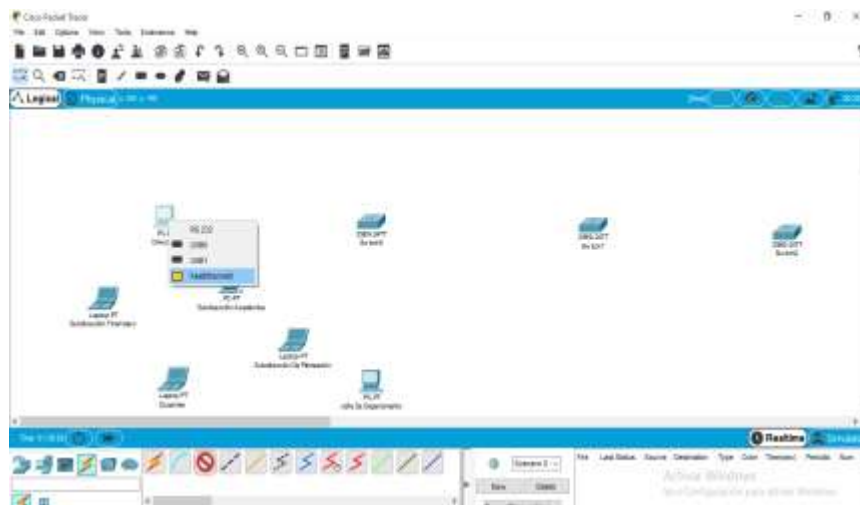
El primer paso para realizar la practica debemos de ingresar los componentes que vamos a utilizar para ello nos dirigimos en la parte inferior izquierda en ella encontramos todos los componentes que necesitamos en este caso los routers, Switchets, los tipos de cables, y las computadoras.



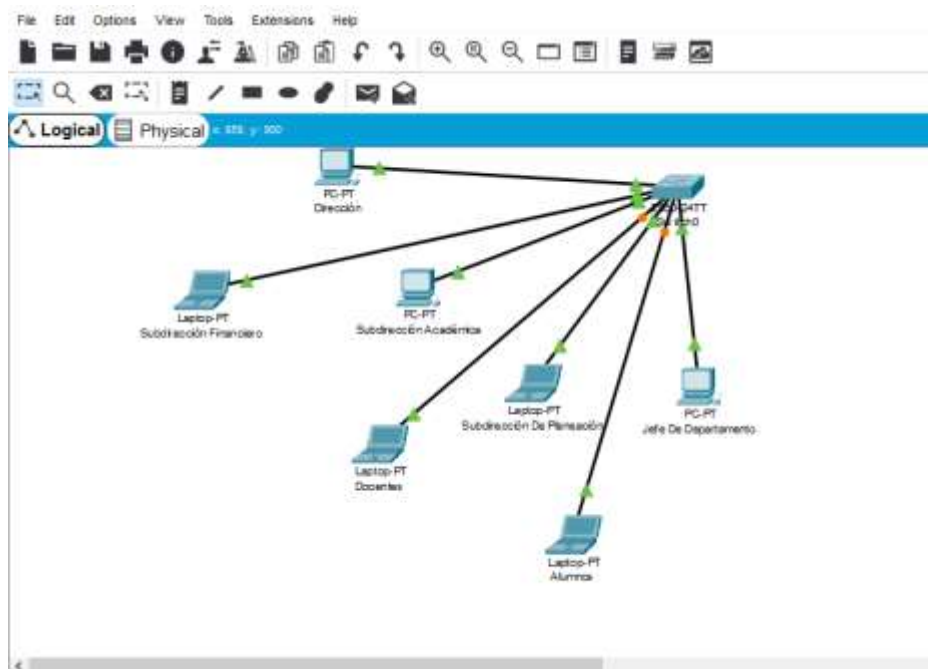
Como segundo paso una vez que hayamos ingresado los componentes a utilizar el paso siguiente es conectarlo por medio de cable desde la pc1 a nuestro Switch esto lo debemos de hacer para todos los equipos clientes que tengamos.



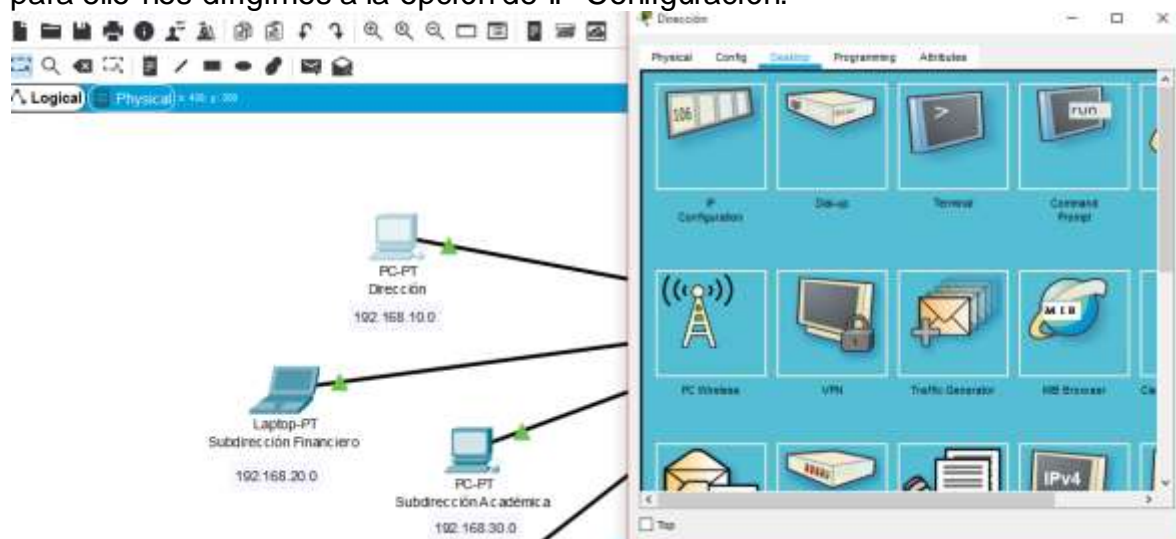
Una vez que hayamos seleccionado el tipo de cable pasamos a conectarlo de pc a switch de acuerdo en que puerto lo queramos conectar.



Una vez que hayamos acabado de conectar los equipos clientes a nuestro switch nos quedara de la siguiente manera.



Como paso siguiente a cada equipo cliente debemos de asignarlo una dirección IP para ello nos dirigimos a la opción de IP Configuración.



The screenshot displays the Cisco Packet Tracer software interface. On the left, a network topology is visible with three devices connected to a central switch:

- PC-PT Dirección** (IP: 192.168.10.11)
- Laptop-PT Subdirección Financiero** (IP: 192.168.20.21)
- PC-PT Subdirección Académica** (IP: 192.168.30.21)

On the right, the **Dirección** (Configuration) window is open, showing the **IP Configuration** tab. The configuration for the selected interface is as follows:

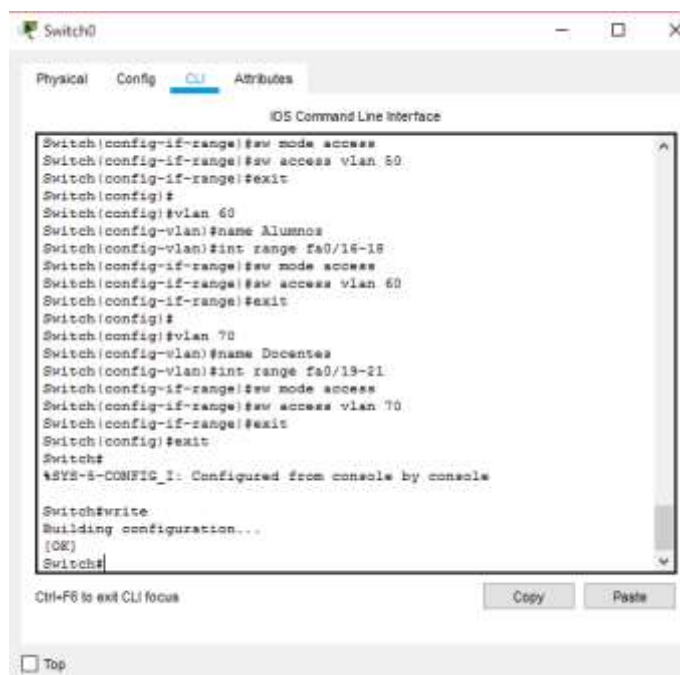
Interface	FastEthernet0/0
IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IP Address	192.168.10.11
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DNS Server	0.0.0.0
Pv6 Configuration	
<input type="radio"/> Automatic	<input checked="" type="radio"/> Static
Pv6 Address	
Link Local Address	FE80::20F:FEBE::C6B
Default Gateway	
DNS Server	
IPv6 TX	
<input type="checkbox"/> Use IPv6 Security	

[illegible]

The diagram on the left shows a central switch labeled 'S24TT' with multiple ports. Several lines represent connections to other devices, some of which are labeled 'S24TT' and 'S24TH'. The terminal window on the right shows the following configuration commands:

```
Switch>enable
Switch>config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# vlan 10
Switch(config-vlan)#name Classroom
Switch(config-vlan)#exit
Switch(config-if-range)#interface fastEthernet 0/24
Switch(config-if-range)#mode access
Switch(config-if-range)#access vlan 10
Switch(config-if-range)#exit
Switch(config)#
Switch(config)# vlan 20
Switch(config-vlan)#name Teachers
Switch(config-vlan)#exit
Switch(config-if-range)#interface fastEthernet 0/24
Switch(config-if-range)#mode access
Switch(config-if-range)#access vlan 20
Switch(config-if-range)#exit
Switch(config)#
Switch(config)# vlan 30
Switch(config-vlan)#name Academic
Switch(config-vlan)#exit
Switch(config-if-range)#interface fastEthernet 0/24
Switch(config-if-range)#mode access
Switch(config-if-range)#access vlan 30
Switch(config-if-range)#exit
Switch(config)#
Switch(config)# vlan 40
```

Una vez ingresado todos los comandos ahora pasamos a utilizar el comando Write este comando nos sirve para guardar toda nuestra configuración.



Para ver como quedo nuestra configuración con las vlan asignadas utilizaremos el comando Show vlan al momento de ingresar este comando podemos ver que nos aparece toda la información de como nosotros hemos asignado los rangos a cada equipo cliente.

Switch0

Physical Config **CLI** Attributes

IOS Command Line Interface

```

Switch-S-CONFIG_1: Configured from console by console

Switch#write
Building configuration...
[OK]
Switch#show vlan

VLAN Name                Status    Ports
-----
1    default                active    Fa0/22, Fa0/23,
Fa0/24, Gig0/1|
10   Direccion               active    Fa0/1, Fa0/2, Fa0/3
20   Financiero              active    Fa0/4, Fa0/5, Fa0/6
30   Academico               active    Fa0/7, Fa0/8, Fa0/9
40   Plneacion               active    Fa0/10, Fa0/11,
Fa0/12
50   Departamento            active    Fa0/13, Fa0/14,
Fa0/15
60   Alumnos                 active    Fa0/16, Fa0/17,
Fa0/18
70   Docentes                 active    Fa0/19, Fa0/20,
Fa0/21
1002 fddi-default            active

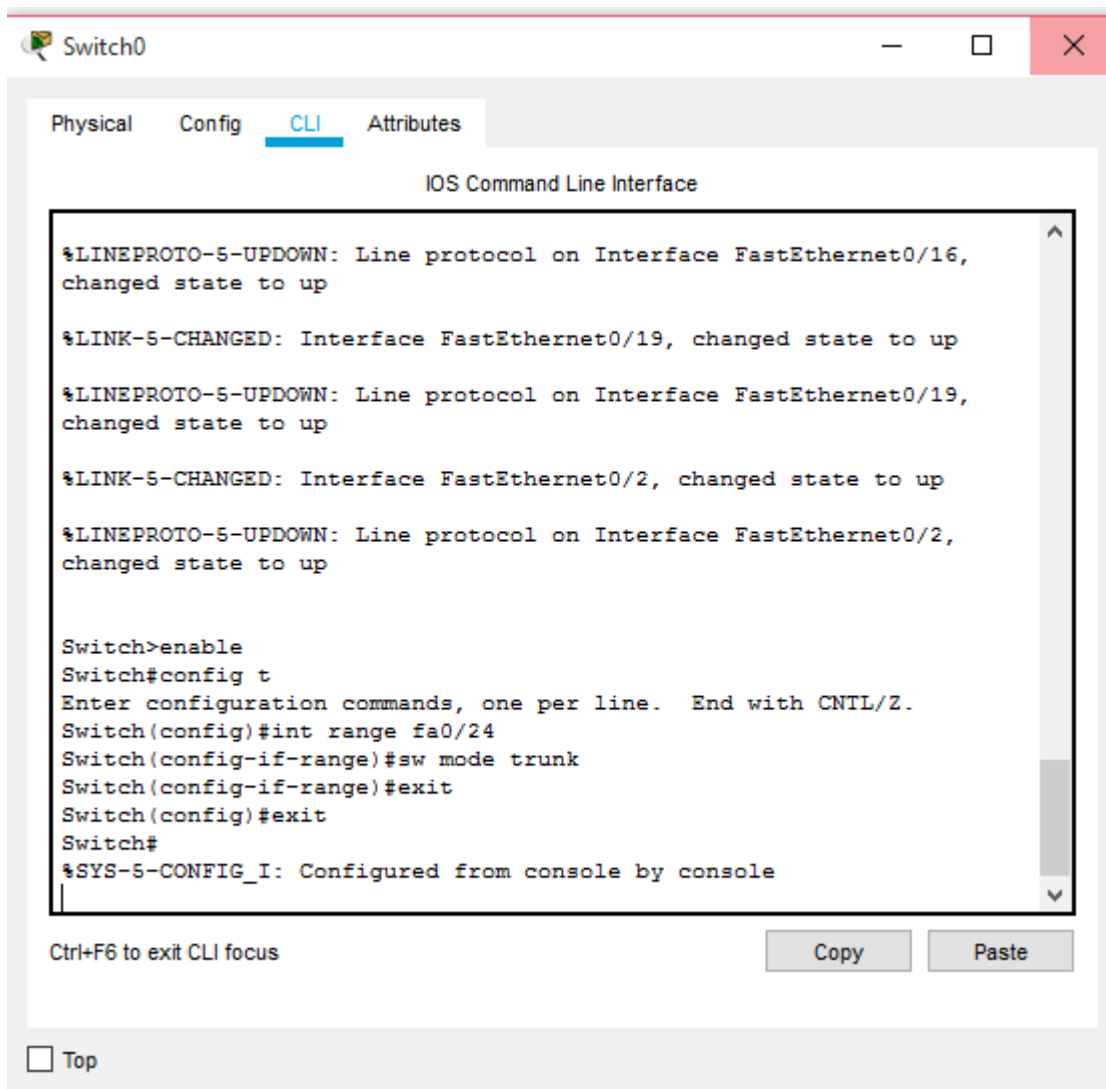
```

Ctrl+F6 to exit CLI focus

Copy Paste

☐ Top

Como paso siguiente procedemos a indicarle cual es el puerto que será el modo Trunk para que de switch a otro switch se puedan enviar paquetes a las diferentes redes que vallamos a agregar esto debemos de hacerlo en cada switch.



```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/16,
changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/19,
changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2,
changed state to up

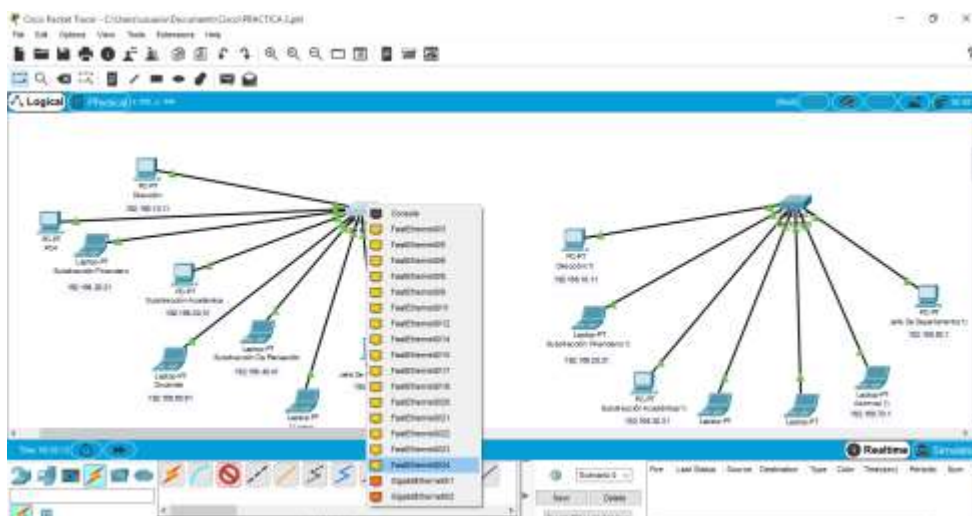
Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int range fa0/24
Switch(config-if-range)#sw mode trunk
Switch(config-if-range)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

Ctrl+F6 to exit CLI focus

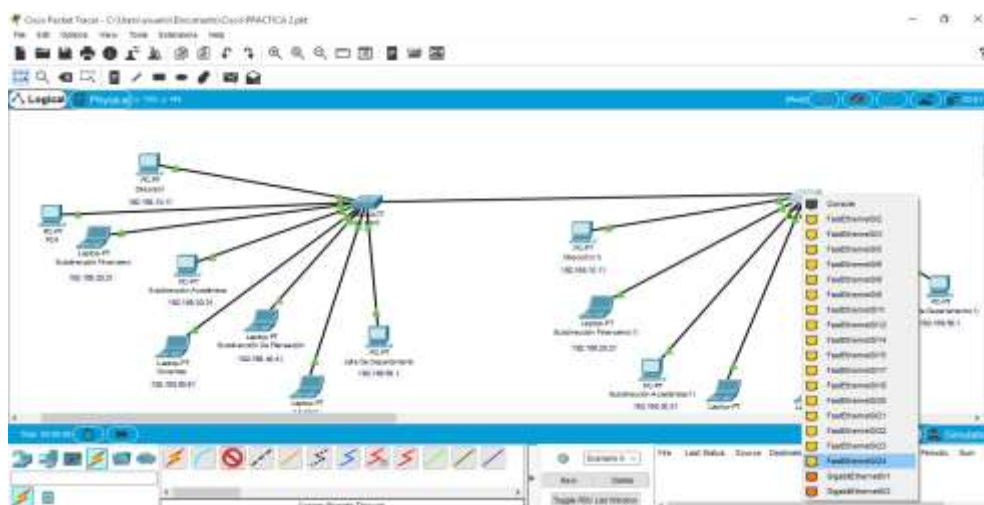
Copy Paste

☐ Top

Como paso siguiente debemos de conectar los switch para ello debemos de seleccionar el tipo de cable y dar clip en el switch y de la lista que nos aparece dar clip en Fa0/24.

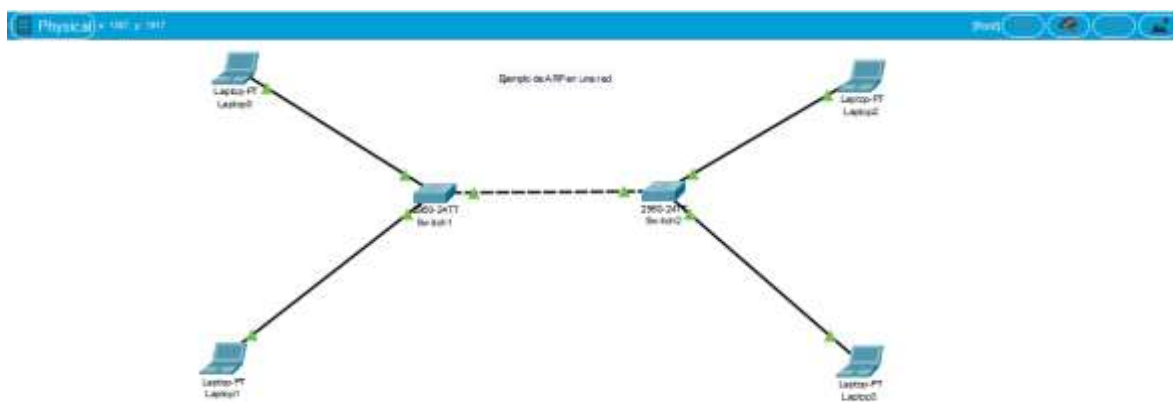


De igual manera en el otro switch debemos de dar clip en Fa0/24 esto lo debemos de hacer con las demás redes que hemos ingresado.

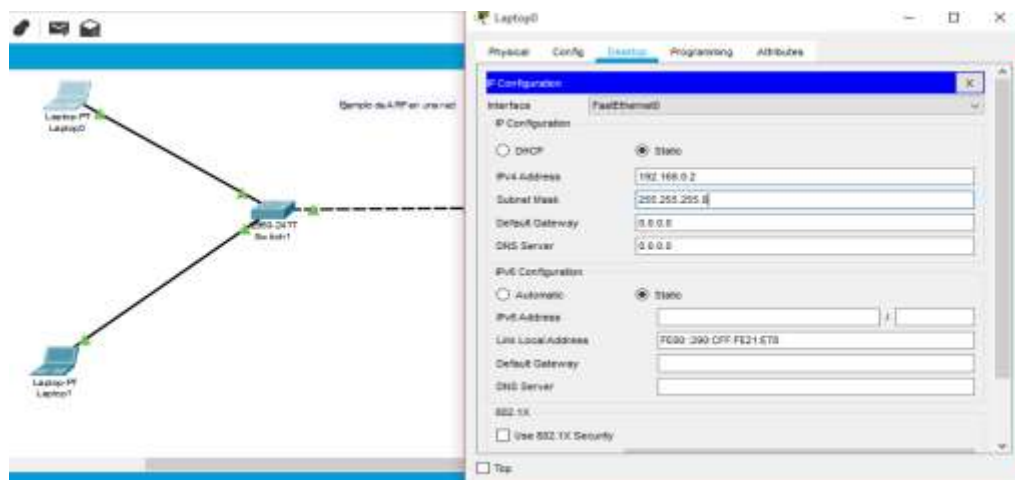


2.-Ejemplo de práctica de ARP.

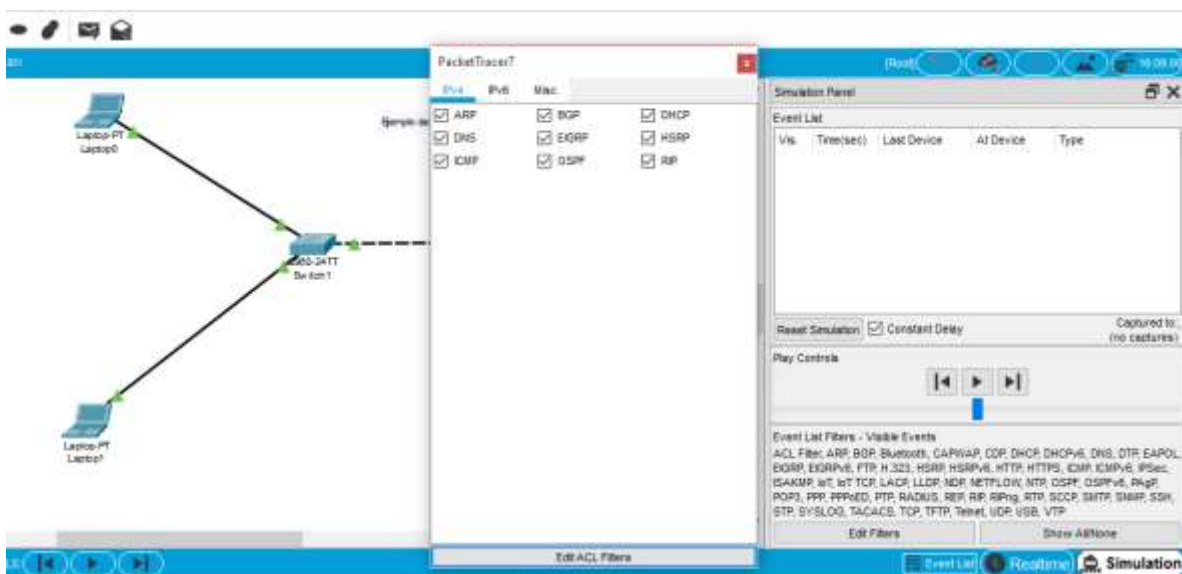
Para realizar esta práctica de ARP debemos de ingresar los componentes a utilizar en este caso son los equipos clientes, switch, tipo de cable lineal y cable cruzado.



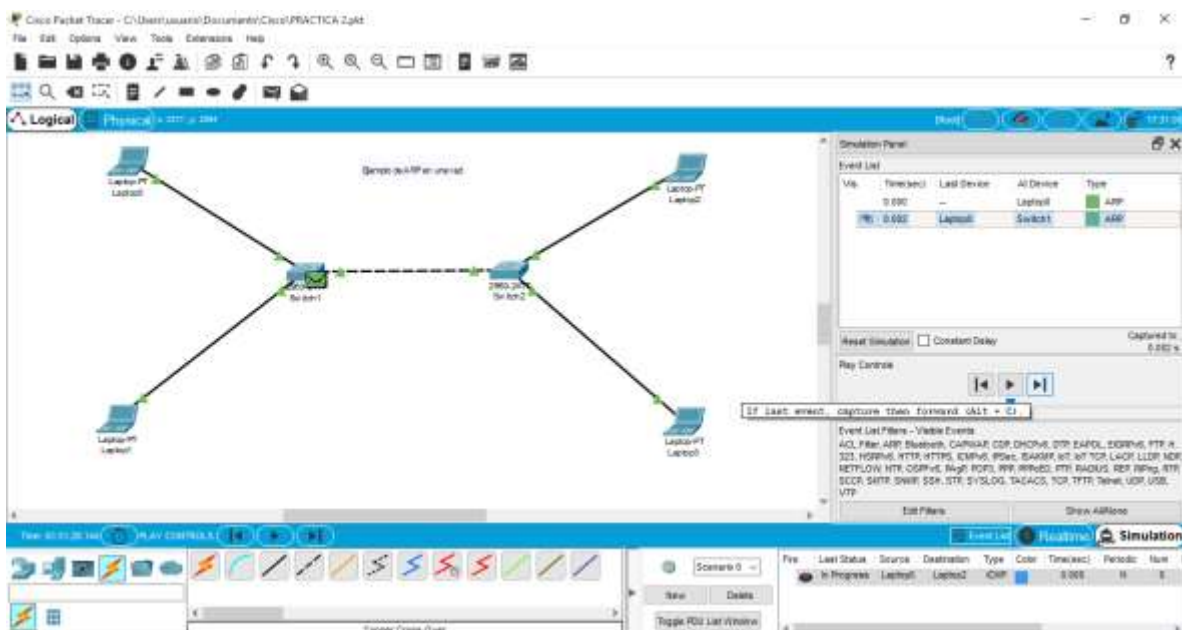
Para continuar con la práctica debemos de ingresarle a cada equipo cliente una dirección IP.



Como paso siguiente debemos de configurar que no estén activados todos los protocolos en este caso no dejaríamos activo la de ARP.



Para realizar las pruebas debemos de mandar un mensaje desde la PC1 a la PC3.



Practica por medio del CMD ARP.

Lo que podemos debemos de hacer es ingresar el comando IP config nos muestra nuestra dirección lógica y física de nuestras diferentes tarjetas ya sea inalámbricas o cableadas.

```
Administrador Símbolo del sistema
Microsoft Windows [Versión 10.0.10240]
(c) 2015 Microsoft Corporation. Todos los derechos reservados.

C:\Windows\system32>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . :

Adaptador de LAN inalámbrica Conexión de área local* 2:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . :

Adaptador de LAN inalámbrica Wi-Fi:

    Sufijo DNS específico para la conexión. . :
    Vínculo: dirección IPv6 local. . . :
    Dirección IPv4. . . . . :
    Máscara de subred. . . . . :
    Puerta de enlace predeterminada. . . :

Adaptador de Ethernet Conexión de red Bluetooth:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . :
```

Como siguiente al momento de escribir el comando arp podemos ver la tabla de conversión de dirección IP que utiliza el comando ARP donde podemos ver las funciones de cada una de ellas ya que funcionan de acuerdo a nuestras necesidades que queramos realizar.

```
Administrador Símbolo del sistema

C:\Windows\system32>arp

Muestra y modifica las tablas de conversión de direcciones IP en direcciones físicas que utiliza el protocolo de resolución de direcciones (ARP).

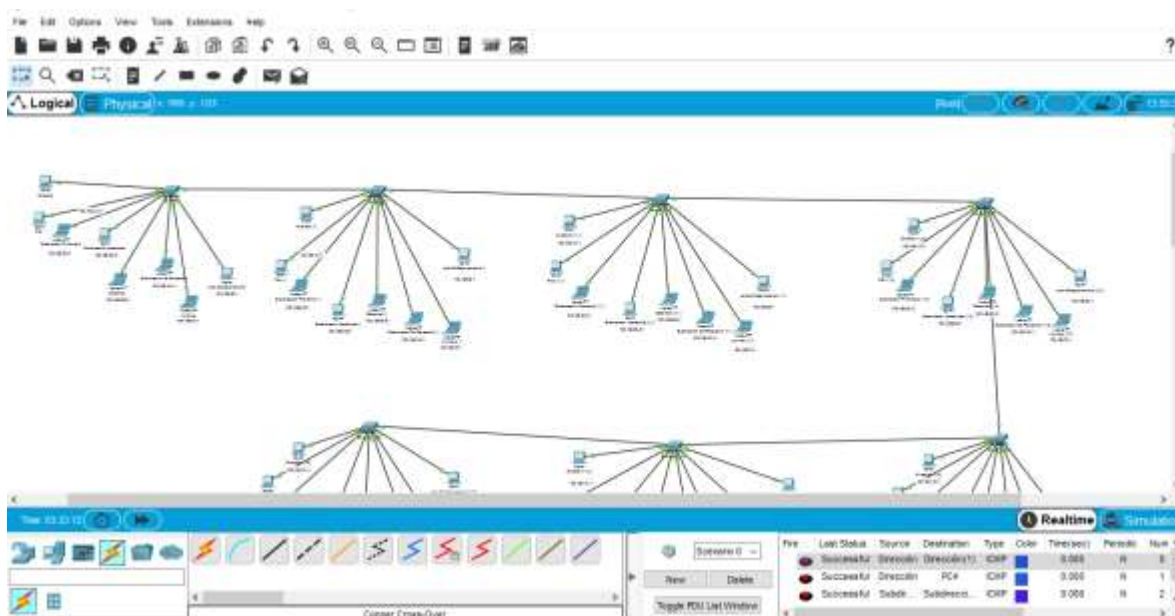
ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

-a      Pide los datos de protocolo actuales y muestra las
        entradas ARP actuales. Si se especifica inet_addr, solo se
        muestran las direcciones IP y física del equipo especificado.
        Si existe más de una interfaz de red que utilice ARP, se
        muestran las entradas de cada tabla ARP.
-g      Igual que -a.
-v      Muestra las entradas actuales de ARP en modo detallado.
        Se mostrarán todas las entradas no válidas y las entradas
        en la interfaz de bucle invertido.
inet_addr Especifica una dirección de Internet.
-N if_addr Muestra las entradas ARP para la interfaz de red especificada
        por if_addr.
-d      Elimina el host especificado por inet_addr. inet_addr puede
        incluir el carácter comodín * (asterisco) para eliminar todos
        los hosts.
-s      Agrega el host y asocia la dirección de Internet inet_addr
        con la dirección física eth_addr. La dirección física se
        indica como 6 bytes en formato hexadecimal, separados por
        guiones. La entrada es permanente.
eth_addr Especifica una dirección física.
```

5.- Resultados

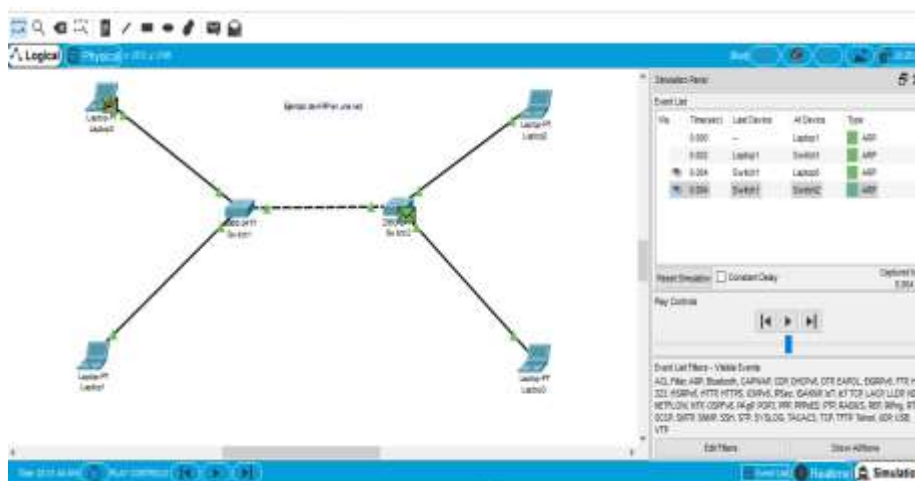
Resultado de la red local a través de VLAN.

Al momento de realizar las pruebas de PC a PC podemos ver que hay comunicación entre ellas ya que se crearon diferentes VLAN ella se pudo observar que si nosotros queremos comunicarnos con otro red donde se encuentre una VLAN con el mismo nombre y los mismos datos podemos ver que existe comunicación y se puede observar los resultado.

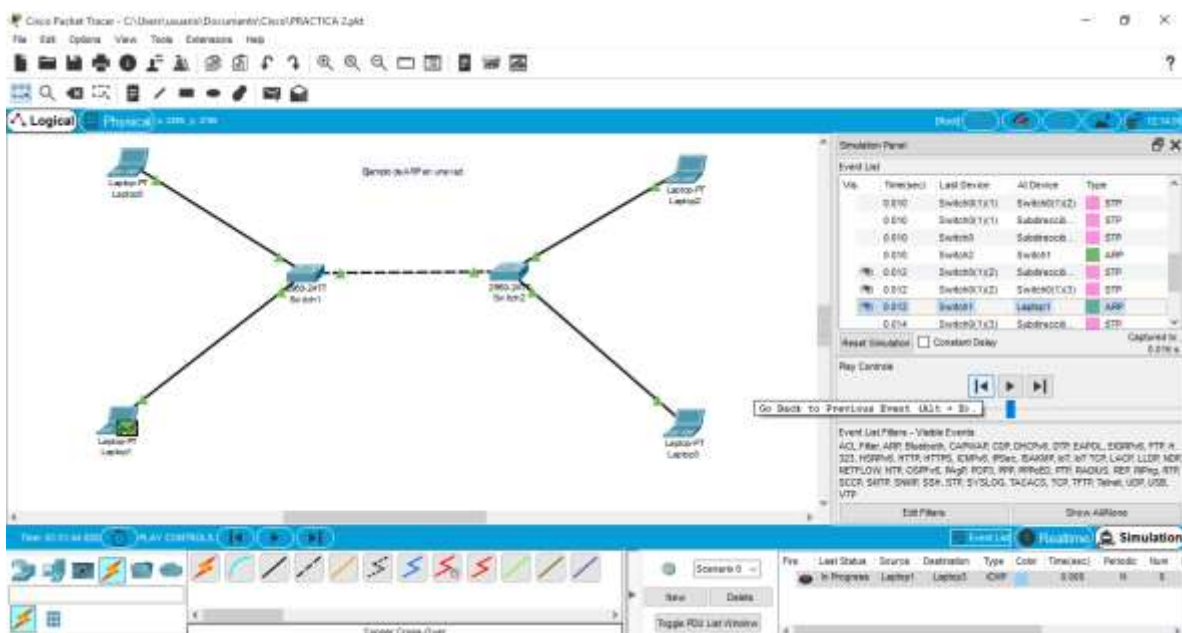
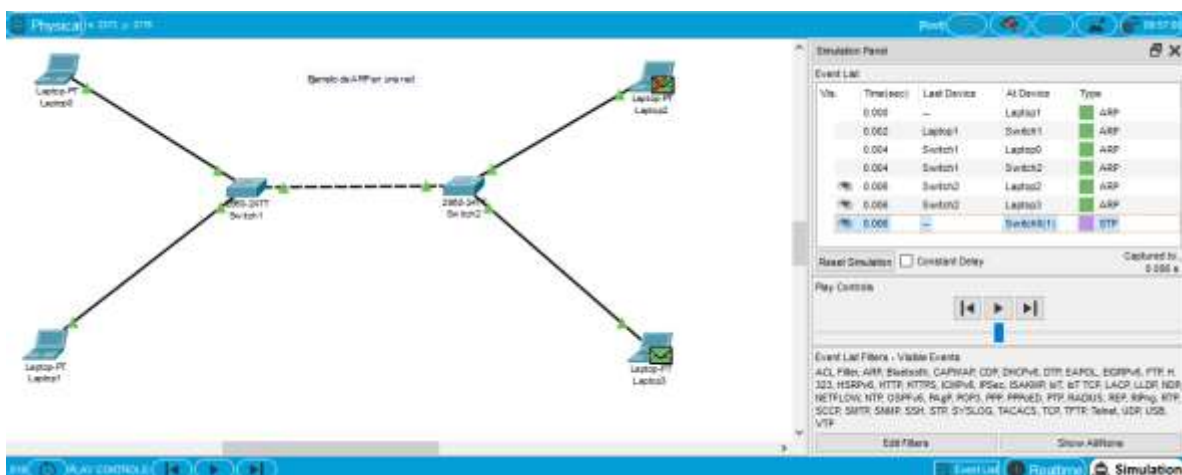


Resultado de Practica de ARP

Como podemos ver en nuestros resultado que al momento de correr nuestro simulador podemos ver que mandara el mensaje al switch y al pc0 y al pc2 ya que esto es porque el ordenador al mandarle el mensaje está haciendo un mensaje de Broadcast ya que solamente conoce la dirección IP destino por lo tanto envía a todos los ordenadores para que le responda al ordenador que tenga la IP destino que el quiere acceder.



Como podemos ver que el mensaje fue llegado a los dos equipos en uno podemos ver que no tiene la dirección IP pero podemos ver que la PC3 responde al mensaje que le mando la PC1 ya que se hizo una solicitud de ARP y de ahí vemos que le devuelve el mensaje con el que le dirá la dirección MAC que tiene ese ordenador para que el ordenador guarde su tabla de ARP ya que fue a la pc que le mando el mensaje.



Resultado del ARP por medio del CMD

Al momento de escribir el comando arp -a este comando nos mostrara la tabla y con ello todos los dispositivos que tenemos conectados.

```
Administrador: Símbolo del sistema

los host.
-s          Agrega el host y asocia la dirección de Internet inet_addr
            con la dirección física eth_addr. La dirección física se
            indica como 6 bytes en formato hexadecimal, separados por
            guiones. La entrada es permanente.
eth_addr    Especifica una dirección física.
if_addr     Si está presente, especifica la dirección de Internet de la
            interfaz para la que se debe modificar la tabla de conversión
            de direcciones. Si no está presente, se utilizará la primera
            interfaz aplicable.

Ejemplo:
> arp -s          .... Agrega una entrada estática
> arp -a          .... Muestra la tabla ARP

C:\Windows\system32>arp -a

Interfaz: --- 0xa
Dirección de Internet      Dirección física      Tipo
                           dinámico
                           dinámico
                           estático
                           estático
                           estático
                           estático
                           estático
```

6.- Conclusiones

En esta práctica realizada entendí como funciona el ARP en una red en este caso se realizó una práctica en el simulador que tenemos de ahí comprendimos que por medio del comandos podemos ver las funciones que nos ofrece el comando, con de igual manera una práctica que se vio de la red del tecnológico superior de chicontepec donde se crearon vlan y en ella realizamos las configuraciones para que cada equipo se comunicara con la vlan que le corresponde al momento de ingresar más equipos clientes podemos ver que tiene comunicación ya que se encuentra en el rango que nosotros establecimos para que exista esa comunicación.

Bibliografía

Cabacas, T. (4 de Marzo de 2019). *MC*. Obtenido de Qué es y para qué sirve la dirección MAC:
<https://www.muycomputer.com/2019/03/04/direccion-mac/>

Diana Hwang. (s.f.). *ComputerWeekly.es*. Obtenido de Red de área local o LAN:
<https://www.computerweekly.com/es/definicion/Red-de-area-local-o-LAN>

Digital Guide. (s.f.). Obtenido de ¿Qué es Ethernet (IEEE 802.3)?:
<https://www.ionos.mx/digitalguide/servidores/know-how/ethernet-ieee-8023/#:~:text=Ethernet%20fue%20desarrollado%20a%20principios,convirti%C3%B3%20en%20un%20producto%20estandarizado.>

Espinosa, O. (05 de mayo de 2022). *Redes Zone*. Obtenido de Switch vs Hub: principales características, diferencias entre ellos y usos:
<https://www.redeszone.net/tutoriales/redes-cable/switch-vs-hub/>

Espinosa, O. (05 de mayo de 2022). *Redes Zone*. Obtenido de Switch vs Hub: principales características, diferencias entre ellos y usos:
<https://www.redeszone.net/tutoriales/redes-cable/switch-vs-hub/>

Jiménez, J. (24 de mayo de 2022). *Redes Zone*. Obtenido de Protocolo ARP: Qué es el protocolo ARP y cómo funciona en redes IPv4

Redes de computadoras. (s.f.). Obtenido de Capa 1 y Capa 2:
<https://sites.google.com/site/investigacionesitlm/4-tecnologia-ethernet/4-1-2-capa-1-y-capa-2>

Redes de computadoras. (s.f.). Obtenido de Control de enlace lógico: conexión con las capas superiores: <https://sites.google.com/site/investigacionesitlm/4-tecnologia-ethernet/4-1-3-control-de-enlace-logico-conexion-con-las-capas-superiores>

Tech Club. (s.f.). Obtenido de Diferencias entre transmisiones Unicast, Multicast y Broadcast.:
<https://techclub.tajamar.es/unicast-multicast-broadcast/>

Wikipedia. (s.f.). Obtenido de Capa física de Ethernet:
https://es.wikipedia.org/wiki/Capa_f%C3%ADsica_de_Ethernet#:~:text=La%20capa%20f%C3%ADsica%20de%20Ethernet,capa%20f%C3%ADsica%20del%20est%C3%A1ndar%20Ethernet.&text=La%20capa%20f%C3%ADsica%20de%20Ethernet%20evolucion%C3%B3%20sobre%20un%20considerable%20pe



TECNOLÓGICO
NACIONAL DE MÉXICO



VERACRUZ
GOBIERNO
DEL ESTADO



SEV
ESTADO DE VERACRUZ

VER Educación
SECRETARÍA DE EDUCACIÓN