INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE COMPUTO

PRACTICA 2

HUBS Y SWITCHES

NOMBRE DEL ALUMNO: GARCÍA QUIROZ GUSTAVO IVAN

GRUPO: 5CV4

NOMBRE DEL PROFESOR: ING. JUAN J. ALCARAZ TORRES

MATERIA: REDES DE COMPUTADORAS

14/10/2023

Introducción

Un hub es un dispositivo de Capa 1 simple que se usa para conectar dispositivos. Cuando un hub recibe una trama en cualquier puerto la envía desde todos los otros puertos. El switch opera en la Capa 2 y aprende las direcciones físicas de los dispositivos conectados a cada puerto. El switch almacena esta información en una tabla. Si el switch recibe una trama destinada a un dispositivo con una dirección física que se encuentra en su tabla, sólo envía la trama desde el puerto en el que está el dispositivo. En esta actividad se compara el funcionamiento de un hub con el funcionamiento de un switch. Si experimenta un retardo al esperar que la luz del switch cambie de ámbar a verde, alternar 3 ó 4 veces entre los modos de tiempo real y simulación acelerará el proceso.

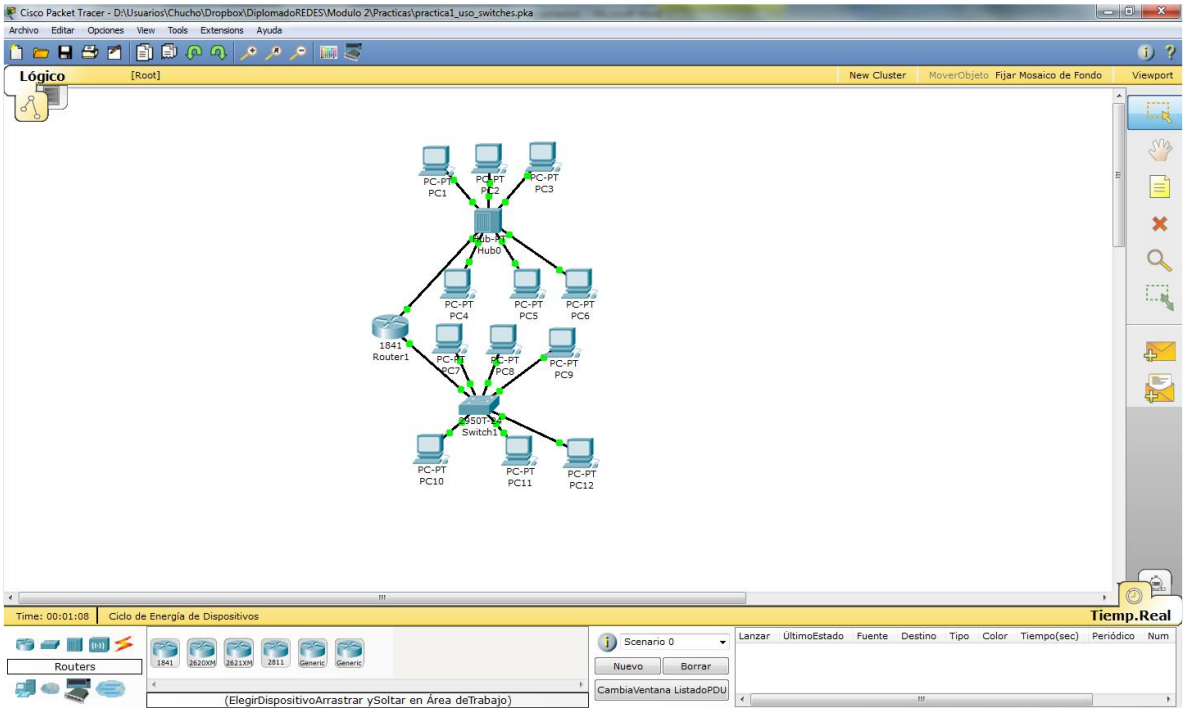


Ilustración 1 Ejemplo de simulacion

Marco Teórico

MAC

La dirección MAC (Media Access Control ó Control de Acceso al Medio), también llamado direccionamiento Ethernet es un conjunto de números binarios de 6 bytes (48 bits) de largo. Pero es representada en 12 dígitos hexadecimales.

Los primeros 3 bytes corresponden al OUI (Identificador Único de la Organización) y los últimos 3 bytes corresponden a un número único e irrepetible que asigna el fabricante.

- Dirección MAC de Broadcast: Las tramas enviadas a una dirección de Broadcast serán enviadas a todos los dispositivos de la red LAN
- Dirección MAC de Multicast: Las tramas enviadas a una dirección de Multicast serán enviadas a

un grupo especifico de dispositivos de la red LAN.

ARP

El protocolo de resolución de direcciones (ARP) es un protocolo que asigna una dirección de protocolo de Internet a una dirección MAC reconocida en la red local. ARP se utiliza para realizar un seguimiento de todos los dispositivos que están conectados directamente a subredes IP del switch.

Por tanto, un paquete IP viaja a través de los dispositivos gracias al descubrimiento de direcciones MAC del protocolo ARP

Para que un router sepa llegar a otro router u otra PC utiliza el protocolo ARP que aprende dinámicamente el direccionamiento de enlace de datos (la MAC de la Capa 2) de una IP de un cliente conectado a la red LAN.

ARP funciona de la siguiente manera:

Se envía un paquete ARP request a la dirección de broadcast (FF:FF:FF:FF:FF:FF) con la dirección
IP por la que pregunta y espera un paquete ARP reply con la dirección MAC que corresponde a esa
IP.

PING

Entender qué es Ping es muy fácil, Ping es un programa usado para diagnóstico de fallas en la red IP usando el paquete ICMP. Cuando hay problemas en la red una de las primeras técnicas que se usa es usar el comando ping para detectar problema, por tanto, el comando ping nos sirve

para aislar las causas del problema e ir segmentando la red hasta encontrar el origen.

El comando ping funciona de la siguiente manera:

Prueba la conectividad enviando paquetes a una dirección IP, esperando que los paquetes vuelvan desde esa dirección de vuelta. El comando envía paquetes que significan “si recibe este paquete, y está dirigido a ti, envía una respuesta”.

Cada vez que el comando ping envía uno de estos paquetes y recibe el mensaje enviado por el otro host (el destino), el comando ping sabe que un paquete se generó desde el host de origen al de destino y viceversa. **ICMP**

Protocolo de mensajes de control en Internet, suministra capacidades de control y envío de mensajes. Herramientas tales como PING y tracert utilizan ICMP para poder funcionar, enviando un paquete a la dirección destino específica y esperando una determinada respuesta. ICMP se describe con más detalle más adelante.

El comando ping usa el ICMP, específicamente envía un mensaje de solicitud (echo request) ICMP y recibe mensajes de respuesta de (echo reply) ICMP. ICMP define muchos otros mensajes, pero estos dos mensajes fueron hechos específicamente para pruebas de conectividad por comandos como el ping.

ICMP no se basa en TCP o UDP, y no utiliza cualquier protocolo de capa de aplicación. Funciona como parte de la Capa 3, como un protocolo de control para ayudar a IP ayudando a gestionar las funciones de la red IP.

Dominio de Colisión y de Broadcast

Dominio de Colisión

Básicamente para saber qué es un Dominio de Colisión en redes, pensemos que está implícito en su nombre, es una parte de la red donde colisiones entre dispositivos ocurren. La colisión ocurre cuando dos dispositivos envían información al mismo tiempo en un segmento compartido.

Atrás en el tiempo lo que se utilizaba en una red era un Hub Ethernet, pero a diferencia de un switch Ethernet el primero no interpreta una señal eléctrica entrante como una trama Ethernet como si lo hiciera un Switch. Básicamente un hub es un repetidor, cuando un repetidor recibe una señal eléctrica éste replica la misma por todos sus puertos (a excepción del puerto de ingreso) regenerando la señal.

Dispositivos (Hub, Bridge, Switch, Router) y los Dominios de Colisión:

Cada interfaz de un Switch separa un dominio de colisión.

- Los Bridges utilizan la misma lógica que un switch, cada interfaz separa un dominio de colisión. • Los Routers separan dominios de colisión por cada interfaz
- Los Hubs no separan dominios de colisión.
- Las redes LAN modernas con switches y routers, con full duplex en cada enlace, no tienen dominio de colisión.
- En una red LAN moderna con todos switches y routers, incluso sabiendo que full duplex elimina los dominios de colisión, piensa en cada enlace Ethernet como un dominio de colisión separado cuando sarga la necesidad de solucionar problemas.

Dominio de Broadcast

El Dominio de Broadcast o Dominio de Difusión es un dominio donde un broadcast Ethernet es enviado. Todos los puertos en un hub o switch por defecto pertenecen al mismo dominio de broadcast. Todos los puertos en un router están en diferentes dominios de broadcast y los routers no reenviaran las tramas de broadcast de un dominio a otro.

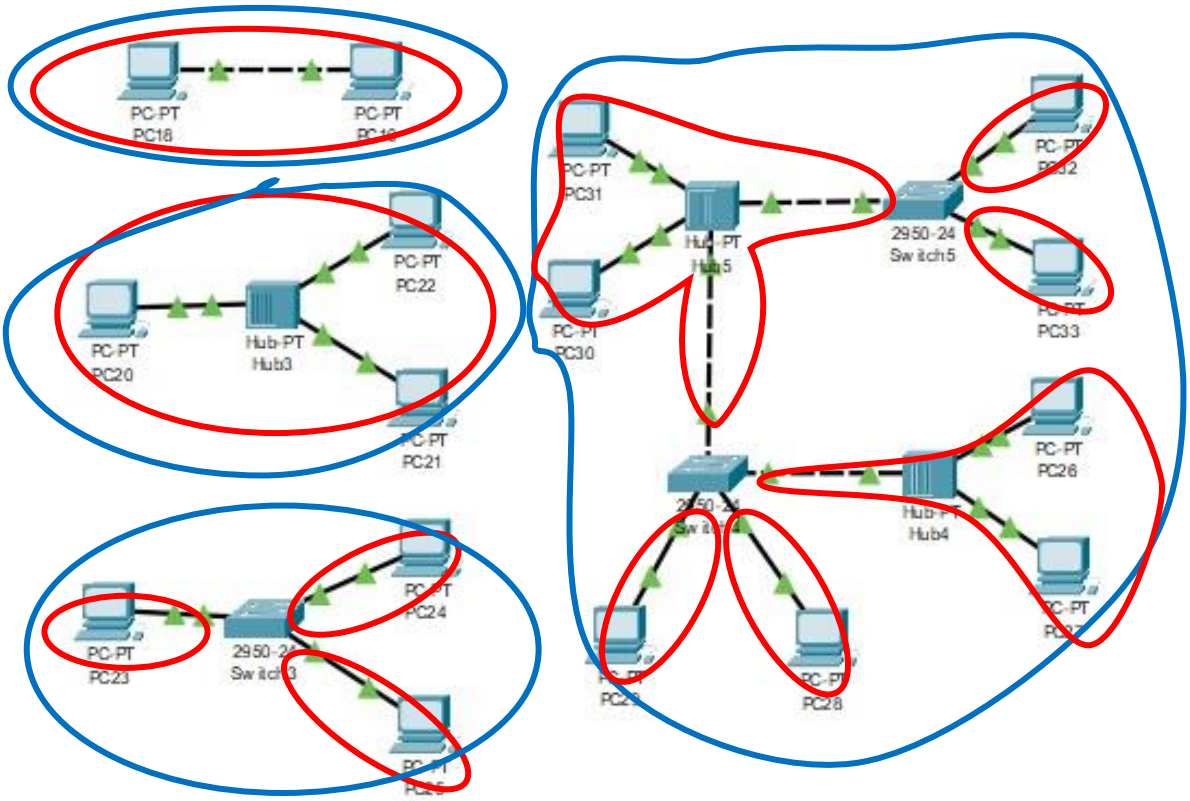
Dispositivos (Switch, Router) y los Dominios de Broadcast:

- Usualmente el único dispositivo que separa dominios de broadcast es el Router.

Para separar dominio de broadcast por medio de un switch, lo que deberíamos hacer es crear VLANs para distintos puertos.

Desarrollo

Realizar el análisis de cada uno de los casos con respecto a la trama Ethernet:



Para el Segundo análisis se requiere escribir en el command prompt de cada pc:

arp -d: Limpia la tabla arp.

arp -a: pantalla de entradas arp.

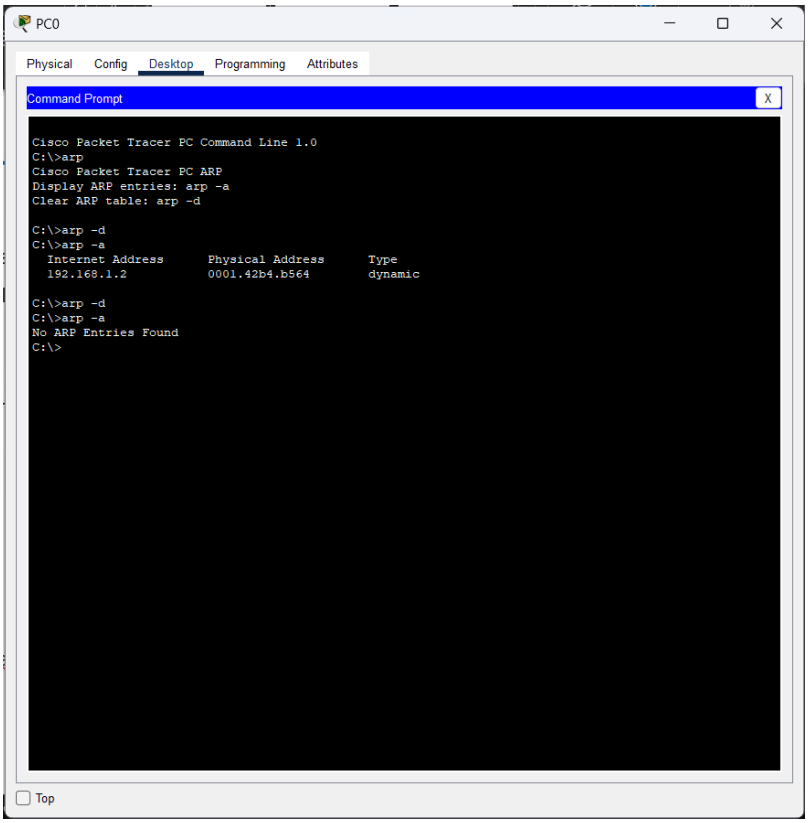


Figure 1 command prompt

Diagrama 1

La siguiente diagrama tiene 2 pc y se envía un mensaje PDU de pc0 a pc1:

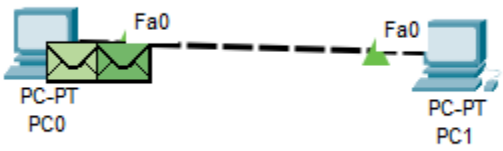


Figure 2 Trama 1

¿Qué es un PDU simple?

Las PDU simples que uno pone en una topología en tiempo real son por defecto un paquete de un protocolo llamado ICMP que complementa las capacidades de IP.

Para la practica se usa ARP.

Trama 1 tiene 1 dominio de colisión y 1 de broadcast y a continuación se tomaron los siguientes datos.

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC0	ICMP
	0.000	--	PC0	ARP
	0.001	PC0	PC1	ARP
Visible	0.002	PC1	PC0	ARP
Visible	0.002	--	PC0	ICMP

Figure 3 Lista de eventos Solicitud de arp

Solicitud de arp

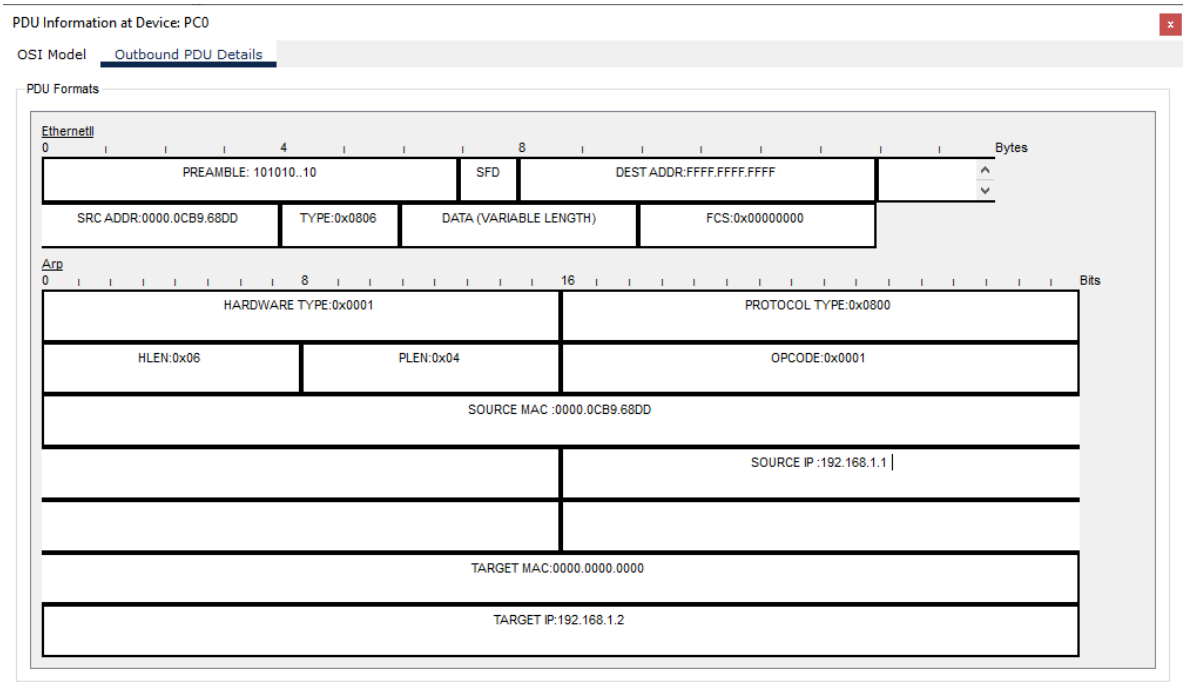


Figure 4 Solicitud de arp Trama 1

En la solicitud de arp podemos ver que lo importante es que lo que se usa en la trama 1, y tiene 1 dominio de colisión y 1 de broadcast y se pasa el PDU de la IP: 192.168.1.1 a IP: 192.168.1.2.

ADDRESS	PC origen	PC destino
IP	192.168.1.1	192.168.1.2
MAC	0000.0CB9.68DD	0000.0000.0000

Respuesta de arp

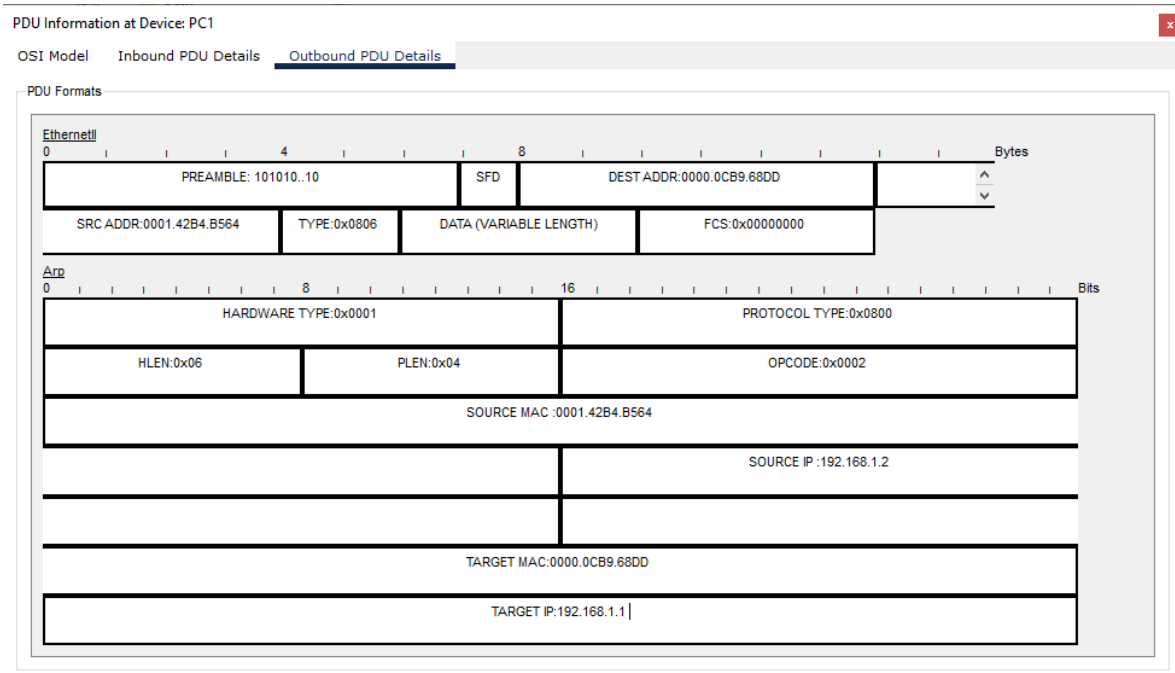


Figure 5 Respuesta de arp Trama 1

ADDRESS	PC destino	PC origen
IP	192.168.1.1	192.168.1.2
MAC	0000.0CB9.68DD	0001.42B4.B564

Diagrama 2

El siguiente diagrama tiene 3 pc y 1 hub y se envía un mensaje PDU de pc2 a pc4:

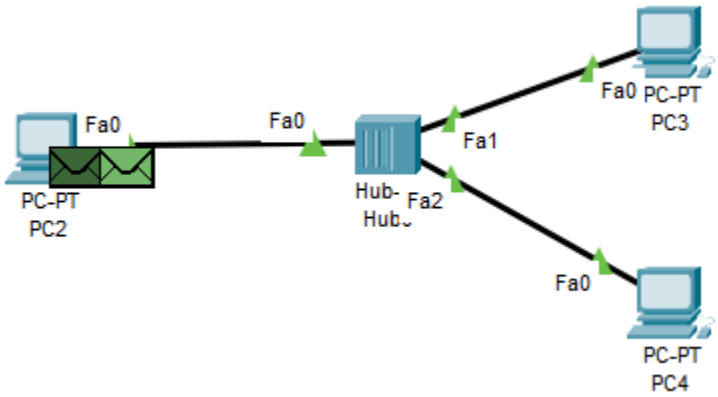


Ilustración 2 Trama 2

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC2	ICMP
	0.000	--	PC2	ARP
	0.001	PC2	Hub0	ARP
	0.002	Hub0	PC3	ARP
	0.002	Hub0	PC4	ARP
	0.003	PC4	Hub0	ARP
Visible	0.004	Hub0	PC2	ARP
Visible	0.004	Hub0	PC3	ARP
Visible	0.004	--	PC2	ICMP

Figure 6 Lista de eventos

Solicitud de arp

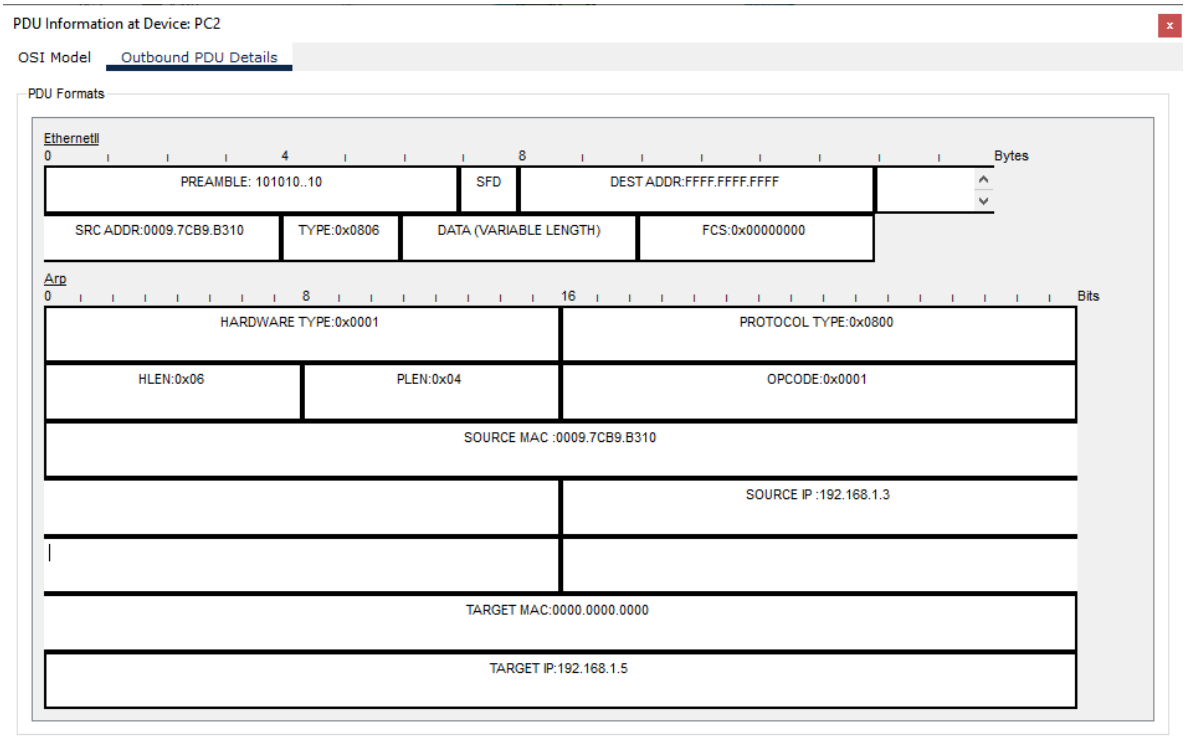


Ilustración 3 Solicitud de arp

En la Solicitud de arp podemos ver que lo importante es que tiene 1 dominio de colisión y 1 de broadcast y se pasa el PDU de la IP: 192.168.1.3 a IP: 192.168.1.5.

ADDRESS	PC origen	PC destino
IP	192.168.1.3	192.168.1.5
MAC	0009.7CB.B310	0000.0000.0000

Respuesta de arp

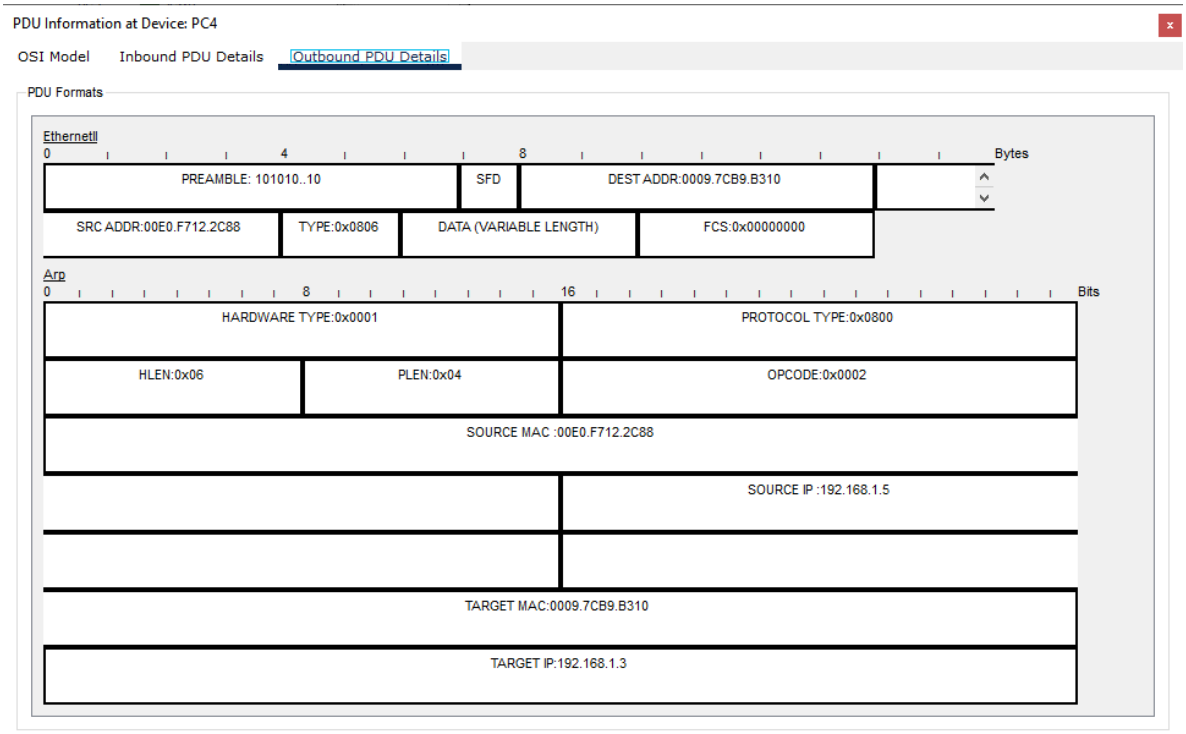


Ilustración 4 Respuesta de arp

ADDRESS	PC destino	PC origen
IP	192.168.1.3	192.168.1.5
MAC	0009.7CB.B310	00E0.F712.2C88

El hub envía la solicitud de pc2 a pc4 y en efecto, si envía de pc2 a pc4, pero notamos que también envía el pc3 y la respuesta de arp pasa de pc2 a pc4 pero también pc3.

Diagrama 3

El siguiente diagrama tiene 3 pc y 1 switch y se envía un mensaje PDU de pc5 a pc7:

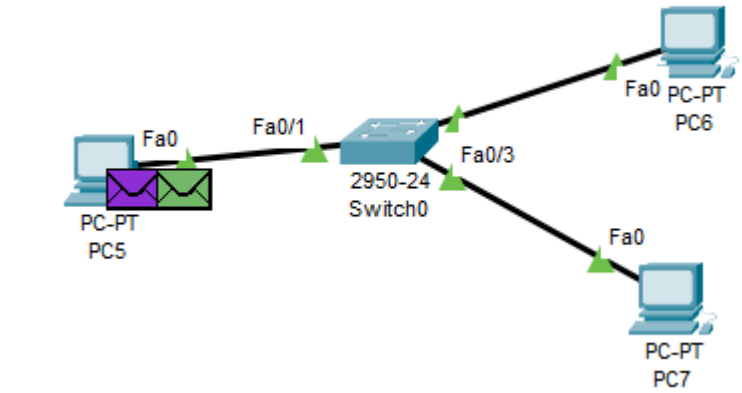


Ilustración 5 Diagrama 3

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC5	ICMP
	0.000	--	PC5	ARP
	0.001	PC5	Switch0	ARP
	0.002	Switch0	PC6	ARP
	0.002	Switch0	PC7	ARP
	0.003	PC7	Switch0	ARP
Visible	0.004	Switch0	PC5	ARP
Visible	0.004	--	PC5	ICMP

Ilustración 6 Lista de eventos

Solicitud de arp

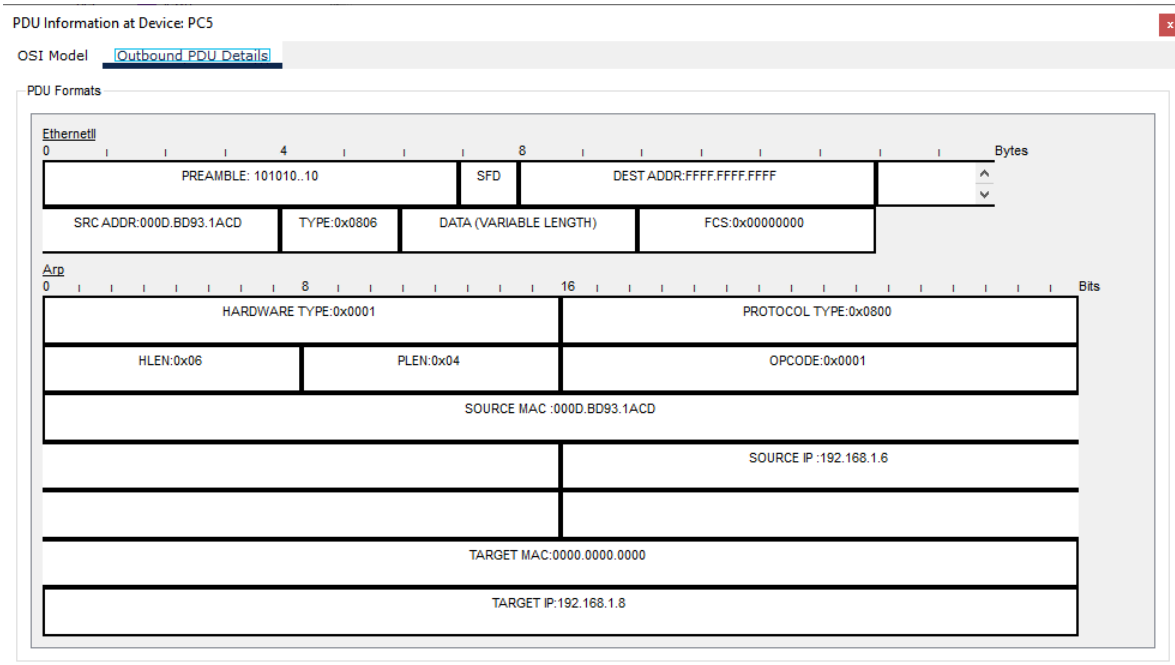


Ilustración 7 Solicitud de arp

En la Solicitud de arp podemos ver que lo importante es que tiene 3 dominio de colisión y 1 de broadcast y se pasa el PDU de la IP: 192.168.1.6 a IP: 192.168.1.8.

ADDRESS	PC origen	PC destino
IP	192.168.1.6	192.168.1.8
MAC	000D.BD93.1ADC	0000.0000.0000

Respuesta de arp

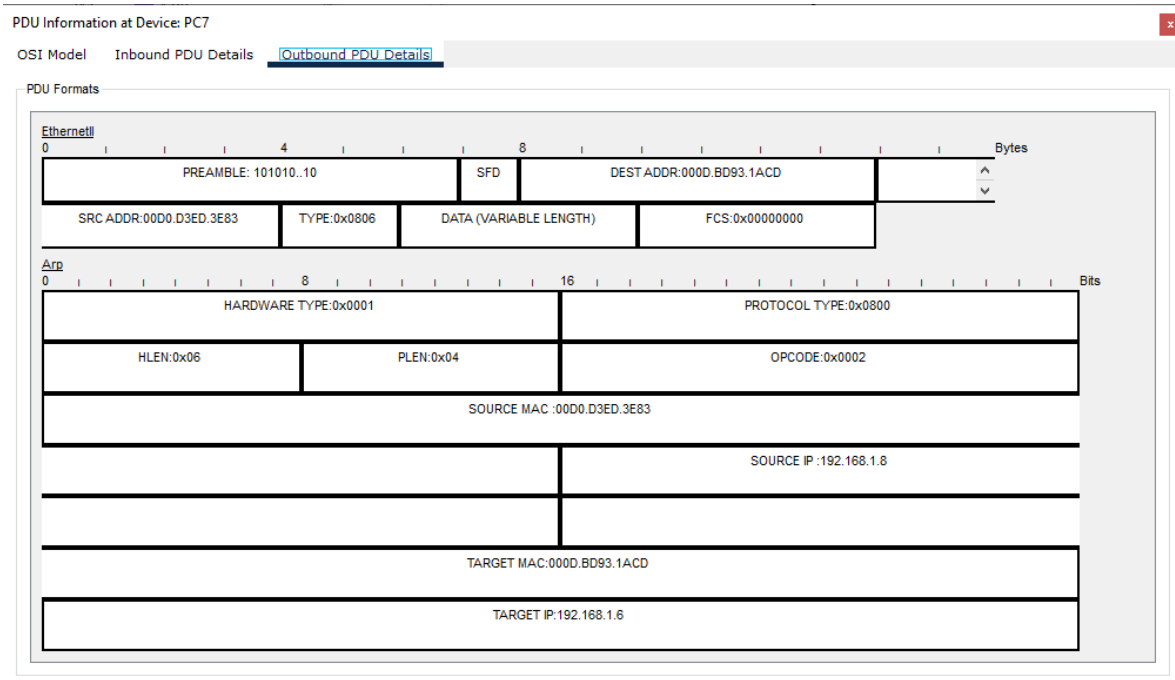


Ilustración 8 Respuesta de arp

ADDRESS	PC destino	PC origen
IP	192.168.1.6	192.168.1.8
MAC	000D.BD93.1ADC	00D0.D3ED.3E83

El switch envía la solicitud de pc5 a pc7 y si envía de pc5 a pc7 pero también pc6 y la respuesta de arp pasa de pc7 a pc5 solamente.

Diagrama 4

La siguiente Trama tiene 8 pc, 2 switch y 2 hub, y se envía un mensaje PDU de pc12 a pc14:

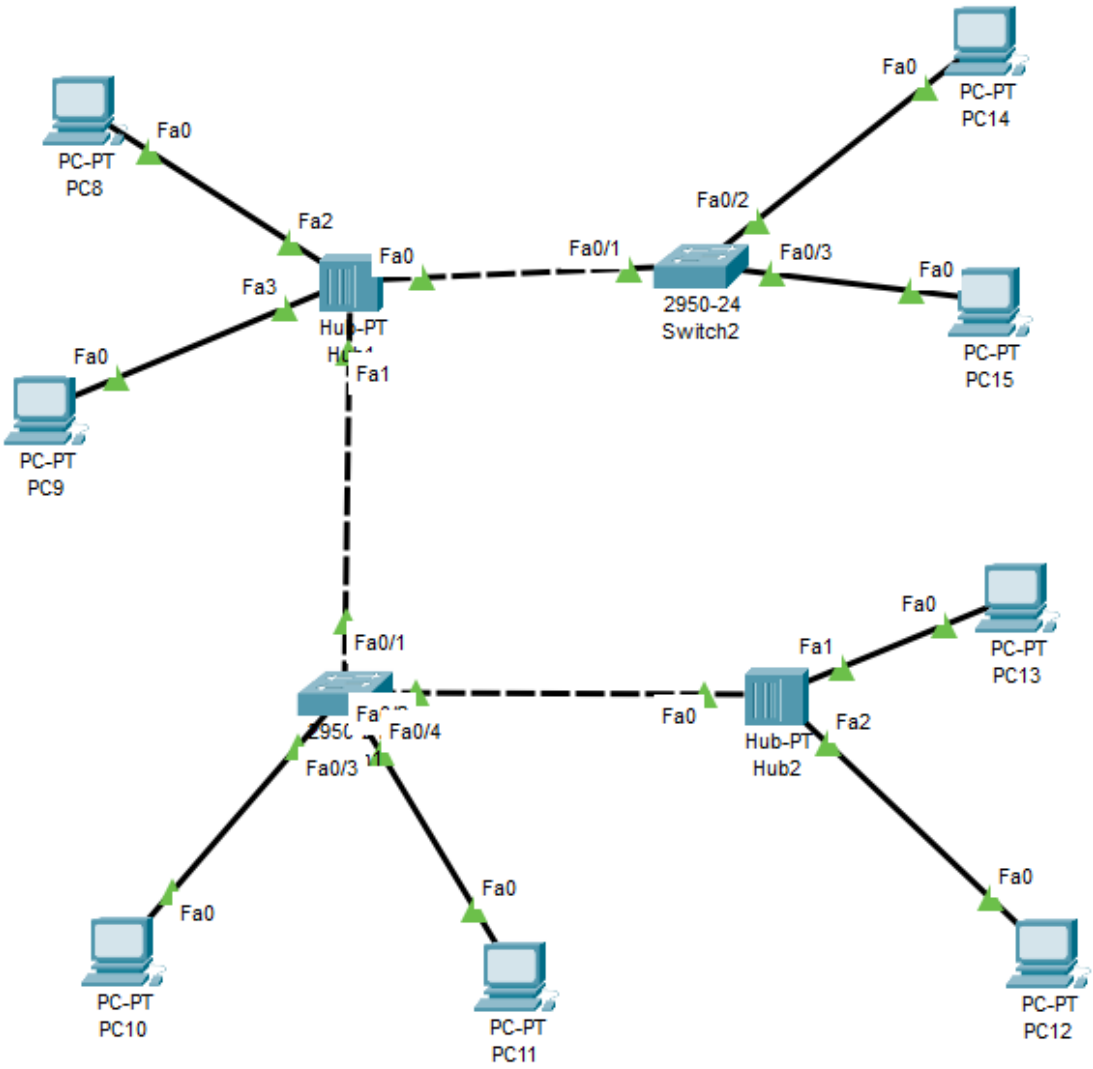


Ilustración 9 Diagrama 4

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC12	ICMP
	0.000	--	PC12	ARP
	0.001	PC12	Hub2	ARP
	0.002	Hub2	Switch1	ARP
	0.002	Hub2	PC13	ARP
	0.003	Switch1	Hub1	ARP
	0.003	Switch1	PC10	ARP
	0.003	Switch1	PC11	ARP
	0.004	Hub1	Switch2	ARP
	0.004	Hub1	PC8	ARP
	0.004	Hub1	PC9	ARP
	0.005	Switch2	PC14	ARP
	0.005	Switch2	PC15	ARP
	0.006	PC14	Switch2	ARP
	0.007	Switch2	Hub1	ARP
	0.008	Hub1	Switch1	ARP
	0.008	Hub1	PC8	ARP
	0.008	Hub1	PC9	ARP
	0.009	Switch1	Hub2	ARP
Visible	0.010	Hub2	PC13	ARP
Visible	0.010	Hub2	PC12	ARP
Visible	0.010	--	PC12	ICMP

Ilustración 10 Lista de eventos

Solicitud de arp

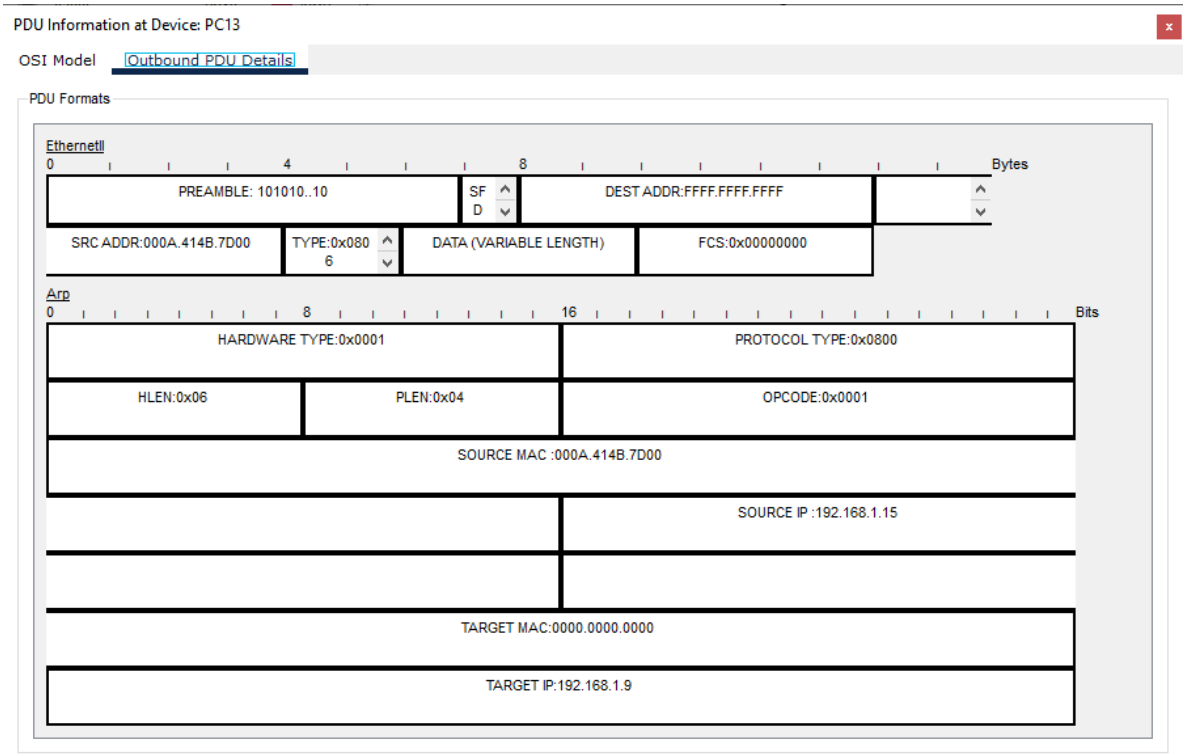


Ilustración 11 Solicitud de arp

En la Solicitud de arp podemos ver que se pasa el PDU de la IP: 192.168.1.15 a IP: 192.168.1.9.

ADDRESS	PC origen	PC destino
IP	192.168.1. 15	192.168.1.9
MAC	000A.414B.7D00	0000.0000.0000

Respuesta de arp

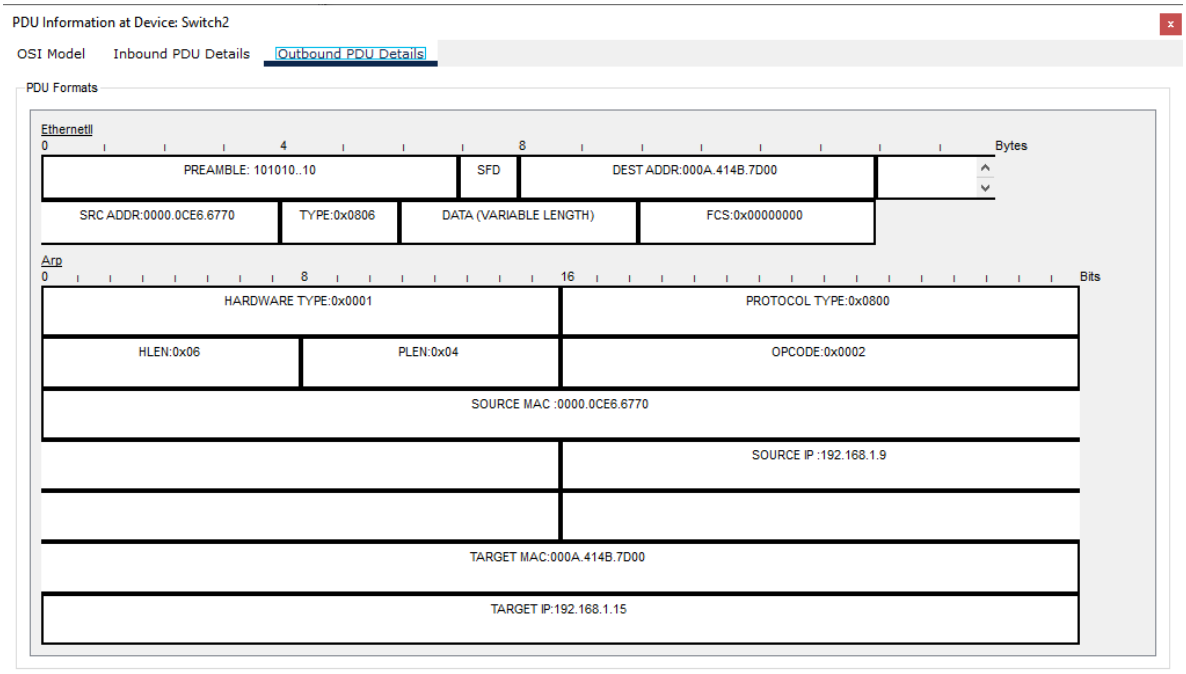


Ilustración 12 Respuesta de arp

ADDRESS	PC destino	PC origen
IP	192.168.1. 15	192.168.1.9
MAC	000A.414B.7D00	0000.0CE6.6770

Conclusión

Como conclusión, los protocolos tienen distintas finalidades. El protocolo ICMP se usa para transmitir mensajes de control y de error entre los dispositivos TCP. Por ejemplo, el comando ping sirve para comprobar si un ordenador está conectado a la red. El protocolo ARP transforma las direcciones IP en direcciones físicas de la capa de enlace. Cada host tiene una tabla para hacer esta transformación. El protocolo ARP es un protocolo estándar específico de las redes, su estado es opcional.

Referencias

- Ariganello, E. (2022). REDES CISCO GUIAS DE ESTUDIO PARA CERTIFICACION CCNA 200 30. Ra-ma.
- CCNA Desde Cero. (2020,). CCNA Desde Cero CCNA 200-301 » Curso Redes Cisco Gratis. https://ccnadesdecero.com/