INSTITUTO POLITECNICO NACIONAL

ESCUELA SUPERIOR DE CÓMPUTO (ESCOM)

REDES DE COMPUTADORAS

NOMBRE DEL ALUMNO:

- SANTOS MÉNDEZ ULISES JESÚS

NOMBRE DEL MAESTRO:

- JUAN JESÚS ALCARAZ TORRES

PRÁCTICA 2:

- HUBS Y SWITCH

Introducción

El Protocolo ICMP

El Protocolo de Mensajes de Control y Error de Internet (ICMP) se encarga de informar al origen si se ha producido algún error durante la entrega del paquete de datos. Pero solo se encarga de notificar los errores, sino que también transporta distintos mensajes de control.

El ICMP en otras palabras se utiliza para comunicar a la fuente original, a los errores encontrados mientras que rutea los paquetes, y a control del ejercicio en el tráfico.

El Protocolo IMCP tiene características similares al UDP (Protocolo de datos de usuario) pero con un formato mucho más simple, su enfoque no está en el transporte de datos, sino en controlar si un paquete no puede alcanzar su destino.

Los mensajes de ICMP requieren doble encapsulación: los mensajes ICMP viajan empaquetados en datagramas IP.

Los mensajes ICMP comienzan con un campo de 8 bits que contiene el tipo de mensaje, el resto de los campos son distintos para cada campo de mensaje ICMP.

Aunque cada tipo de mensaje tiene su propio formato, todos ellos comparten los primeros tres campos:

- Tipo (8 bits)
- Código (8 bits)
- Checksum (16 bits)

¿Cómo trabajan los mensajes de redireccionamiento ICMP?

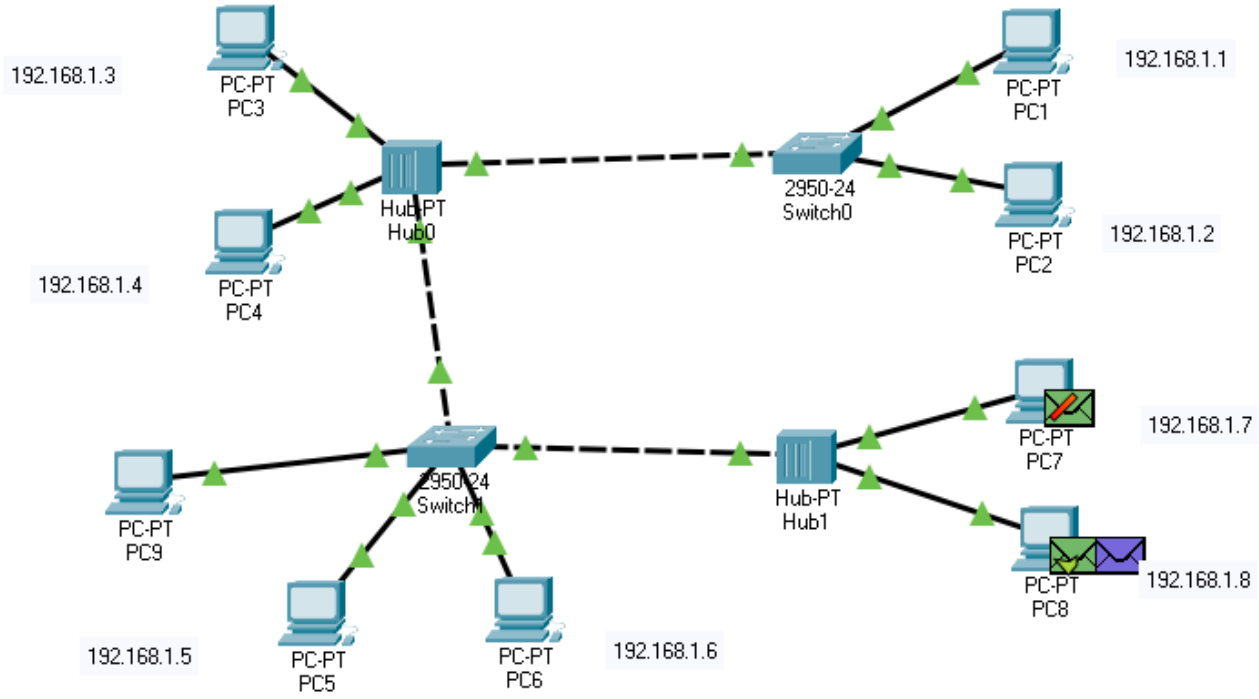
Los routers utilizan los mensajes de redireccionamiento ICMP para informarle a los hosts en el link de datos que está disponible una ruta mejor para un destino particular.

Mensajes informativos del ICMP

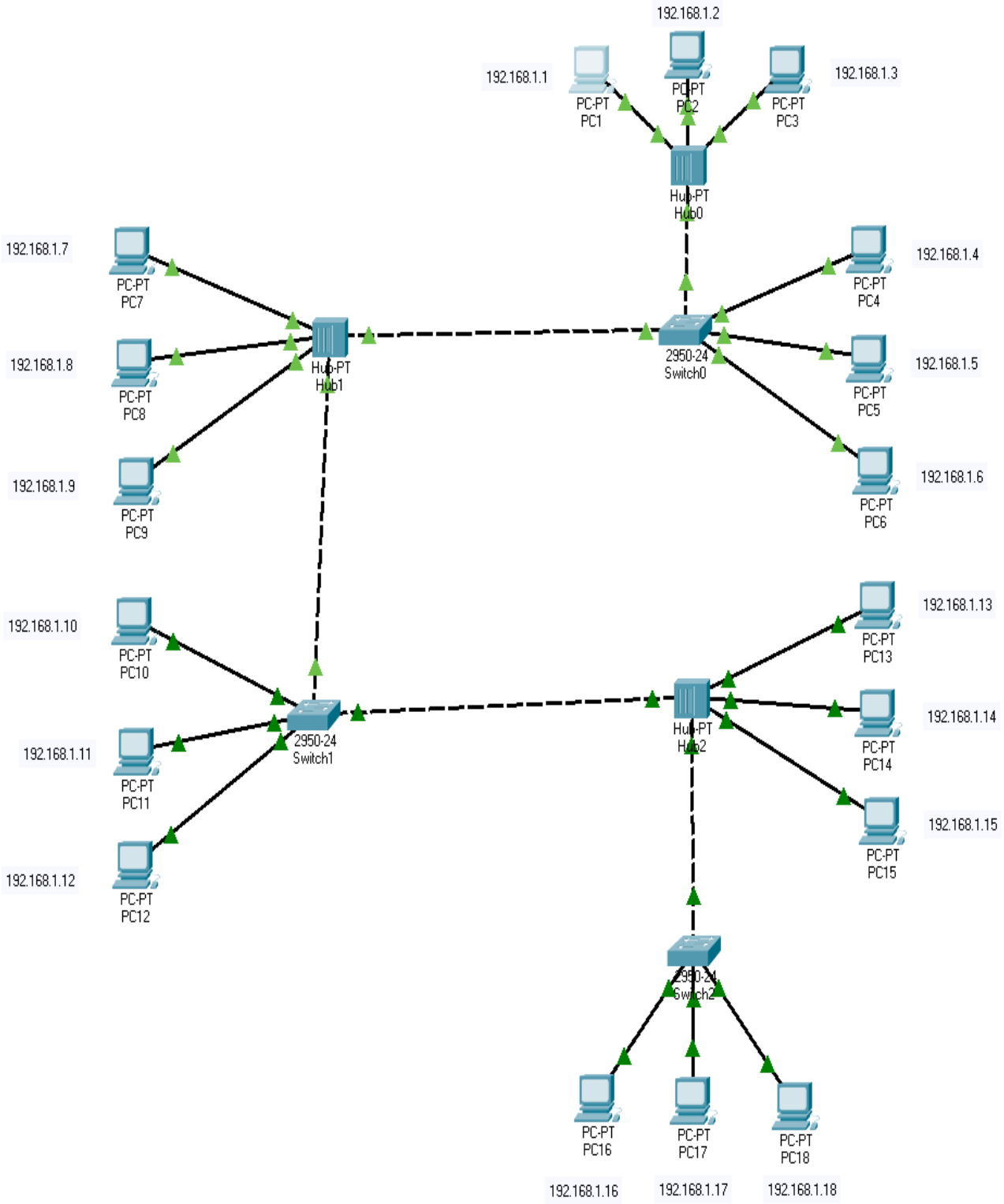
Tipo	Mensaje
0	Echo Reply (respuesta de eco)
3	Destination Unreacheable (destino inaccesible)
4	Source Quench (disminución del tráfico desde el origen)
5	Redirect (redireccionar - cambio de ruta)
8	Echo (solicitud de eco)
11	Time Exceeded (tiempo excedido para un datagrama)
12	Parameter Problem (problema de parâmetros)
13	Timestamp (solicitud de marca de tiempo)
14	Timestamp Reply (respuesta de marca de tiempo)
15	Information Request (solicitud de información) - obsoleto-
16	Information Reply (respuesta de información) - obsoleto-
17	Addressmask (solicitud de máscara de dirección)
18	Addressmask Reply (respuesta de máscara de dirección

Desarrollo

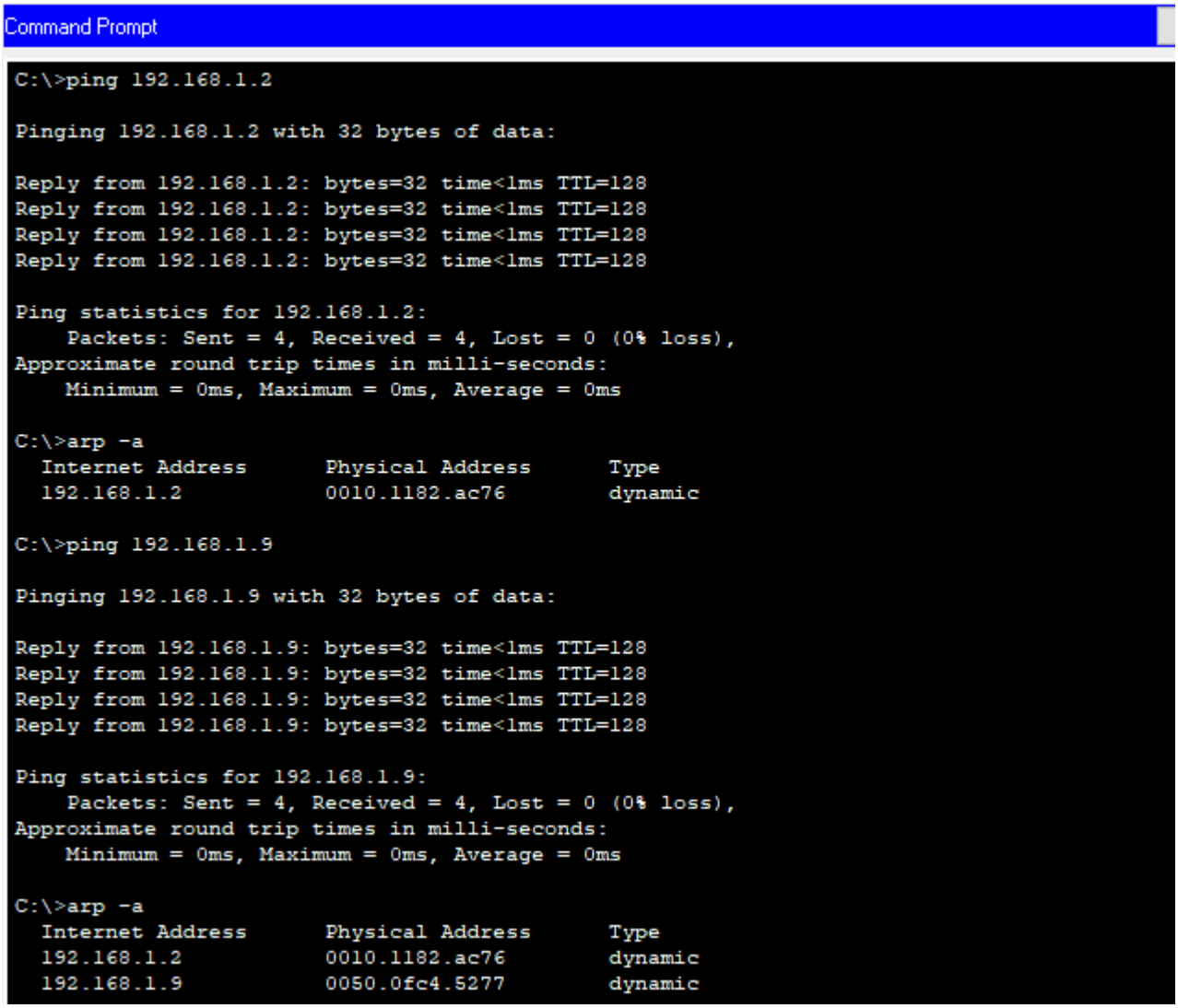
1. Se hizo la construcción de la red que esta como ejemplo previo al problema de la práctica para ver el funcionamiento del hub y del switch, inicialmente se le asigno a cada PC una dirección IP, después se procedió a hacer una simulación de una PC a otra, en este caso fue de la PC8 a la PC9.



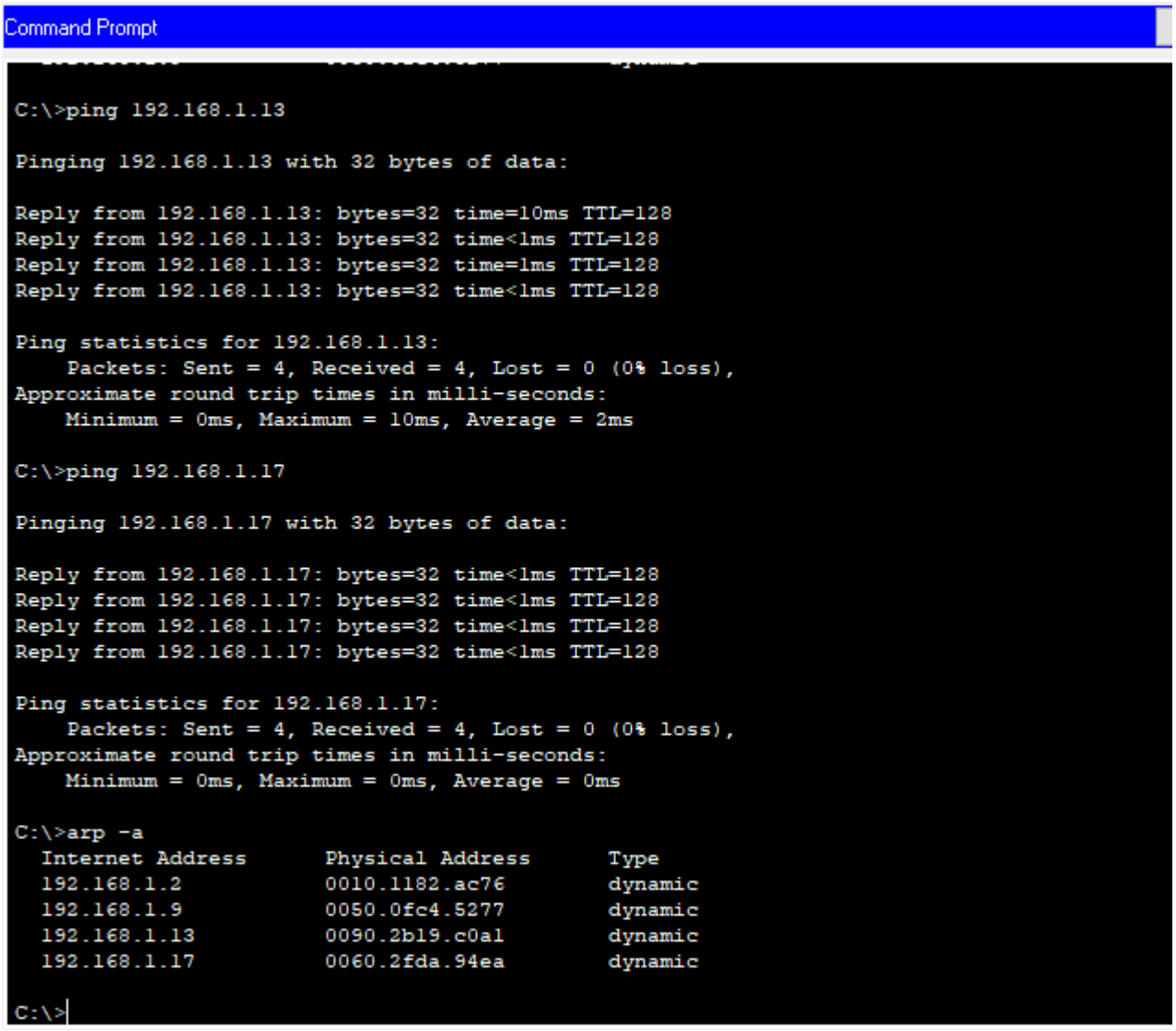
2. Se tiene que hacer el diagrama propuesto en la práctica, al realizar las conexiones con cable se nos comentó que los que van hacia las PC's son con cobre directo y las conexiones de hub a switch o de switch a hub son con cable cruzado, en la construcción se le asigno a cada PC una IP respectiva.



3. Se comprueba con la terminal que se tenga la conexión con las computadoras, se busco ver la conexión correcta con la PC2 y la PC9.



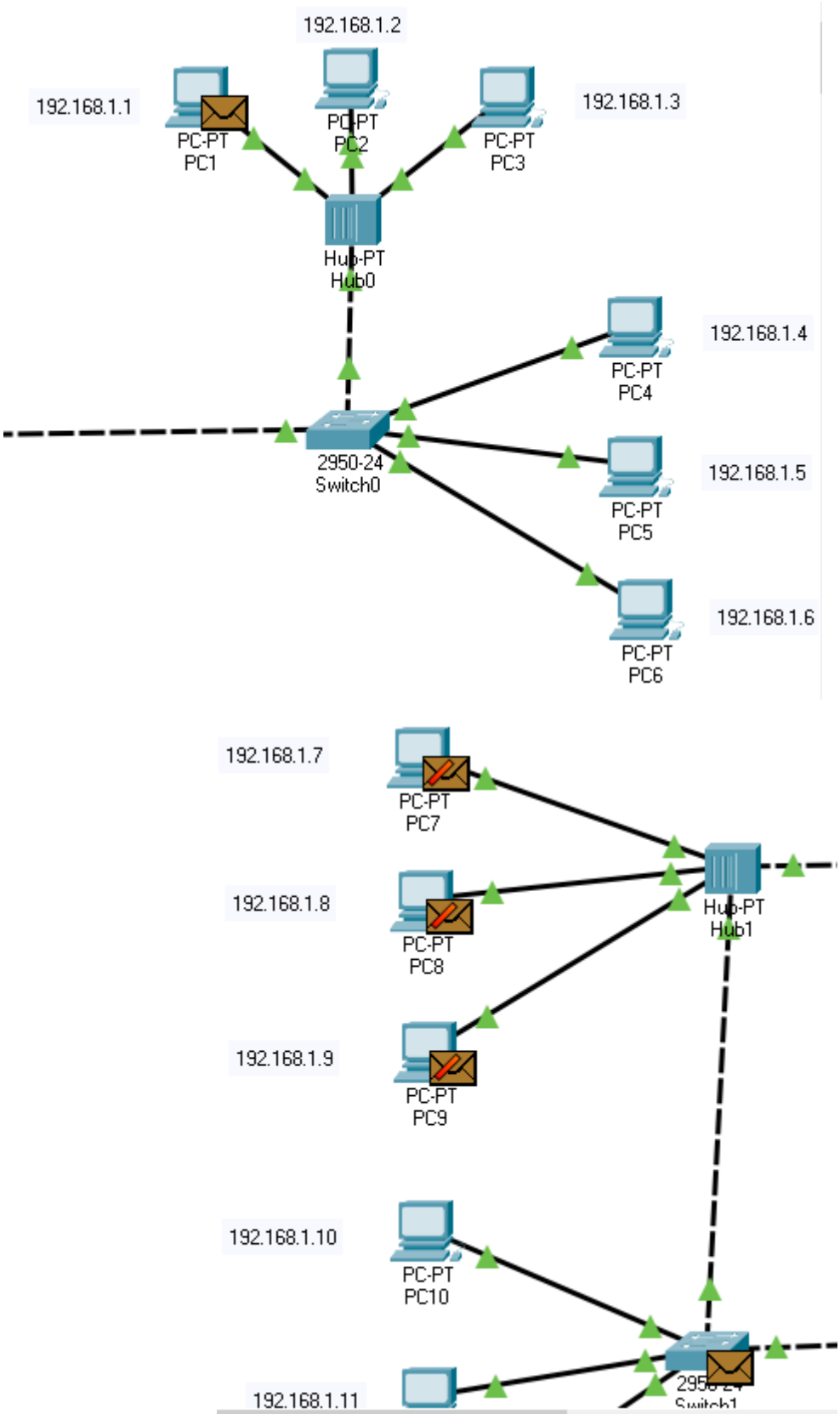
4. Ahora se comprueba la conexión con PC's más lejanas a la PC1, en este ejemplo será comprobar la conexión con la PC13 y la PC17.

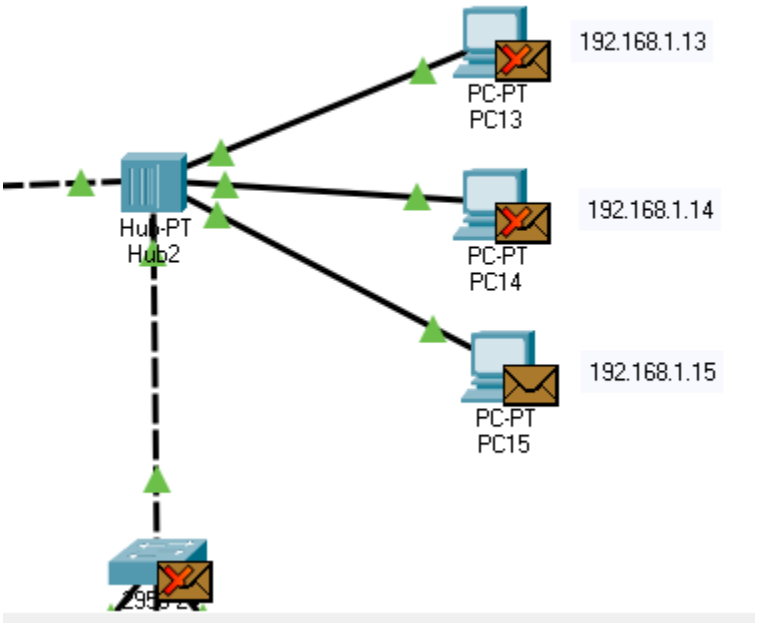


5. Ya comprobada la conexión de la PC1 con las cercanas y lejanas, se procede a realizar una serie de simulaciones.

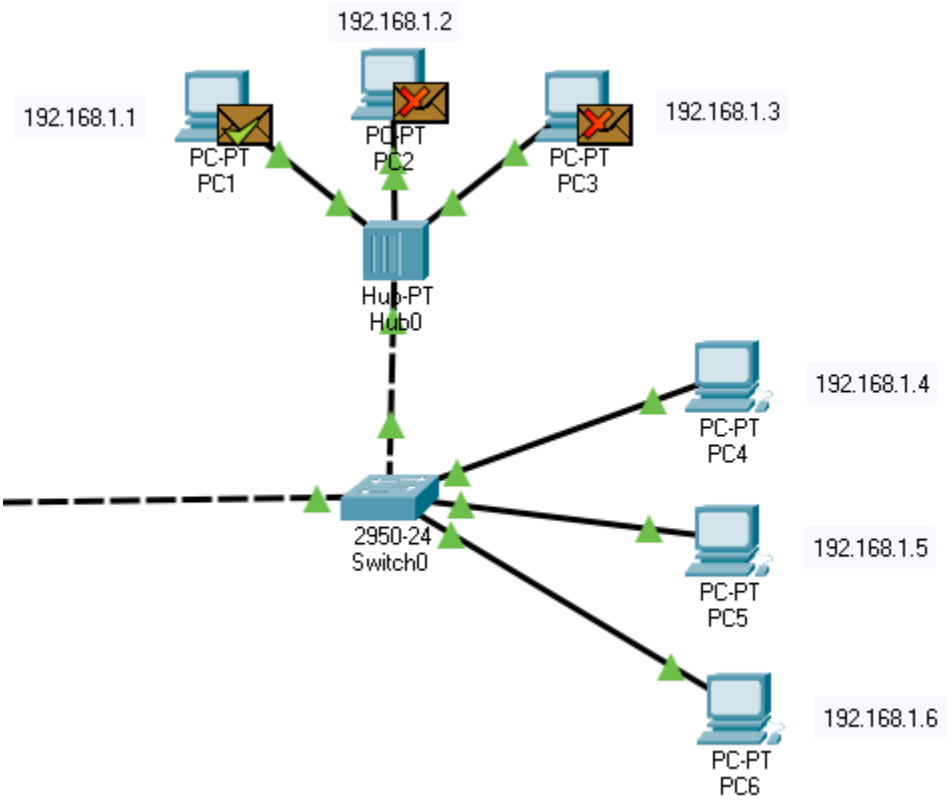
- Simulación: PC1 a PC15

  Los datos pasan de la PC1 al Hub0, después se reparte el paquete datos a la PC2 y PC3 siendo erróneos ya que no es el destinatario, después pasa por el Switch0, del Switch0 se direcciona el paquete en la PC4, PC5, PC6 y el Hub1, siendo erróneos en las PC's porque ninguna es el destino, después pasa por el Hub1, y se dirige el paquete hacia el Switch1 ya que con las demás PC's no se pudo ya que no llevan a ninguna otra dirección tampoco y tampoco son el destino, después pasa por el hub2 y reparte entre las PC's dando a dos erróneas y finalmente llega a la PC15 procesando el paquete de datos.


192.168.1.2
192.168.1.1
192.168.1.3
PC-PT
PC1
PC-PT
PC2
PC-PT
PC3
Hub-PT
Hub0
192.168.1.4
PC-PT
PC4
2950-24
Switch0
192.168.1.5
PC-PT
PC5
192.168.1.6
PC-PT
PC6
192.168.1.7
PC-PT
PC7
Hub-PT
Hub1
192.168.1.8
PC-PT
PC8
192.168.1.9
PC-PT
PC9
192.168.1.10
PC-PT
PC10
192.168.1.11



Se hace el mismo recorrido de vuelta hasta que se manda a la PC1 que el paquete de datos ha sido recibido por la PC15.



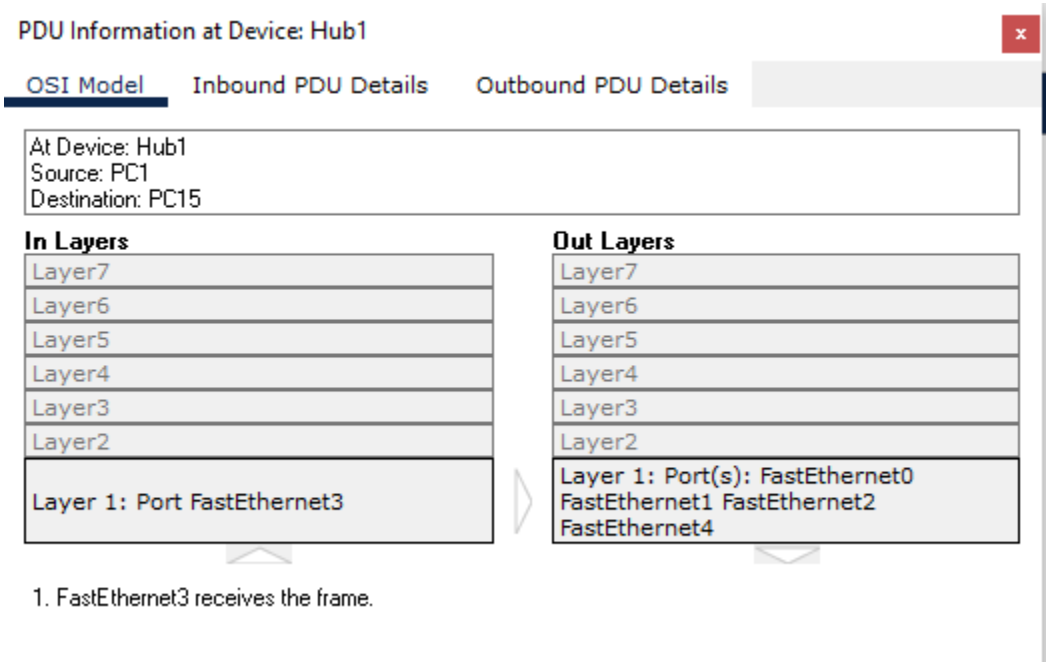
6. Al ingresar el comando ping 192.168.1.15 en la terminal mientras se simula, al llegar el paquete al emisor de nuevo nos dice que hubo respuesta por parte del destinatario.

```
C:\>ping 192.168.1.15

Pinging 192.168.1.15 with 32 bytes of data:

Reply from 192.168.1.15: bytes=32 time=12ms TTL=128
```

7. Al pulsar alguno de los dispositivos en ejecución se puede visualizar que ellos tienen ya la dirección del emisor y la del receptor.



Conclusión

En conclusión, se comprobó el uso y conexión de los switch y hub, también se comprendió como distribuyen los datos, y el uso del ICMP para determinar errores en el envío del paquete, esto tiene una gran relación con los dominios de colisión ya que como se observó en la simulación y en su análisis se reparte el paquete de datos en las PC's dominadas por el switch, se observó cómo es la recepción y el retorno del paquete de datos, siguiendo el camino con ayuda del hub y del switch.