DEPARTAMENTO DE COMPUTACION

Facultad de Ciencias Exactas y Naturales - UBA

TP3: Integración

Teoría de las Comunicaciones

Segundo Cuatrimestre de 2021

Integrante	LU	Correo electrónico
Christian Nahuel Rivera	184/15	christiannahuelrivera@gmail.com
Guido Rodriguez Celma	374/19	guido.rc98@gmail.com
Miguel Rodriguez	57/19	mmiguerodriguez@gmail.com

Facultad de Ciencias Exactas y Naturales

Universidad de Buenos Aires

Ciudad Universitaria - (Pabellón I/Planta Baja)

Intendente Güiraldes 2610 - C1428EGA

Ciudad Autónoma de Buenos Aires - Rep. Argentina

Tel/Fax: (+54 11) 4576-3300

https://exactas.uba.ar

1. Ejercicio 1

1.1. Conexiones físicas y protocolos de nivel de enlace

En el edificio vamos a utilizar conexiones físicas Ethernet a través de cables categoría 5e (hasta 1000 Mbps) con conectores RJ-45 para interconectar a las computadoras con la red interna y poder transmitir datos de manera confiable. Estos tipos de conectores y protocolo son los más utilizados actualmente y la mayoría de las computadoras tienen puertos con este tipo de entradas para hacer interfaz con Ethernet.

Por la forma en que vamos a distribuir los hosts y switches (los hosts se conectan cada uno a un puerto distinto del switch de su piso y los switches se conectan con los del piso superior e inferior) no es necesario usar el protocolo de Spanning Tree (STP) pues el grafo que define la red es acíclico. De este modo lo desactivaremos en nuestros switches.

Vamos a utilizar el protocolo Learning Bridge para evitar tener que configurar manualmente las tablas de forwarding de los switches. Además nuestra red contará con un Router conectado al Switch del primer piso que proveerá conexión a Internet para todo el edificio.

A continuación presentamos un diagrama de cómo quedaría configurada la red para el edificio según lo descripto anteriormente:

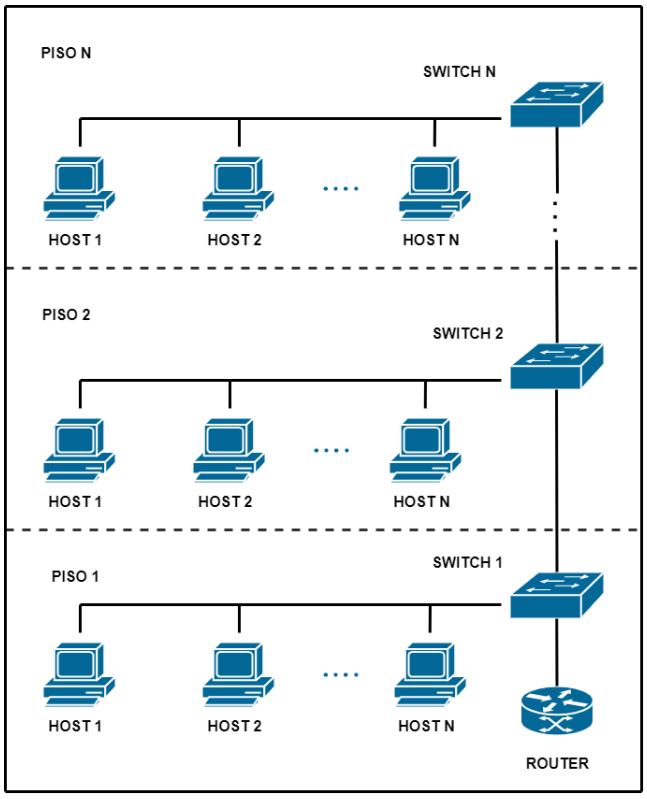

Figura 1: Estructura LAN

En el diagrama podemos observar que por piso proponemos la instalación de un switch que conecte a cada PC a uno de sus puertos. A su vez los switches se van a interconectar entre si.

Para la capa de enlace de datos, usaremos el protocolo punto a punto sobre ethernet (PPPoE por sus siglas en inglés). Este protocolo nos permite que cada PC pueda transferirle información al switch, y luego a otra PC en la red. En este protocolo las conexiones son de a pares PC-switch. Además, los dispositivos que están a ambos extremos del cable envían tramas de información dirigidas a una dirección MAC (dirección única de cada PC). La elección de este protocolo es debido a que está ampliamente soportado por el hardware actual, está creado para transportar información sobre ethernet y nos provee una base sólida para el protocolo que usaremos sobre él, IP.

1.2. Protocolo de red y ruteo

Utilizaremos el protocolo ARP para que los dispositivos puedan comunicarse entre si dentro de la red interna mediante sus direcciones MAC. El protocolo a utilizar sera IPv4 por el hecho de su uso masivo y confiabilidad. Como nuestra red interna consiste de switches con un único router, no es necesario utilizar un protocolo de ruteo de paquetes (como RIP u OSPF) para la comunicación entre hosts.

1.3. Nivel de transporte

Nuestra red debe permitirnos leer los datos de los sensores de manera confiable, tener la posibilidad de recuperarse ante posibles errores y reenviar el estado de los datos en caso de fallas. Es por esto que para el nivel de transporte vamos a utilizar el protocolo TCP. Este protocolo garantiza la confiabilidad y el orden de entrega de un flujo de datos, algo que esperamos para la transmisión de datos dentro de nuestro edificio.

1.4. Capa de aplicación

Los mensajes de capa de aplicación son importantes a la hora de aprovechar el uso de la red dentro del edificio ya que no queremos saturarla con mensajes excesivamente largos. Los programas necesitan poder:

- Descubrir la red. Cada computadora conectada a un sensor debe responder.
- Obtener información de un sensor particular.
- Establecer conexión con una computadora para solicitar información en tiempo real.
- Enviar información de un sensor.

Para el primer item definimos un mensaje `GETSENSORS`, este podrá ser utilizado por cualquier host que quiera obtener información de todos los sensores de la red. El mismo se broadcastea por toda la red; cuando un host lo recibe, si tiene un sensor asociado responde con `GETSENSORSRESPONSE` al host que originó el mensaje indicándole el ID del sensor y su tipo. De esta manera, el host inicial puede almacenar a qué host de la red pertenece cada sensor y la información del mismo.

Una vez obtenida la información de los sensores, un host puede consultar el estado de cualquiera de ellos enviando al host correspondiente un mensaje `GETSENSORSTATUS`. Al recibirlo, el host asociado le envía el estado de su sensor encapsulado en un paquete `SENSORSTATUSRESPONSE` con destino el host que realizo el pedido.

Finalmente, si un host quisiera tener actualizaciones en tiempo real de un sensor particular, puede enviarle al host asociado al mismo un mensaje `GETREALTIMESENSORSTATUS`. Este mensaje podría desencadenar un proceso similar al del algoritmo `three-way handshake` para establecer la conexión. Una vez establecida, el host que tiene el sensor le enviará cada cierto tiempo una actualización del estado del sensor encapsulada en un paquete. Para liberar la conexión, nuevamente se puede utilizar un algoritmo similar al `four-way handshake` entre ambos hosts.

1.5. Seguridad

Como necesitamos tener un router para poder acceder a internet desde nuestra red local, debemos implementar medidas de seguridad para protegernos de que usuarios externos puedan entrar en la red. Para ello pensamos implementar tres medidas muy conocidas y efectivas.

- Firewall
- Usar una NAT en nuestro router
- Filtrado por MAC address

La primera de nuestras estrategias consiste en proteger, desde el único punto de conexión con el mundo exterior, todo tráfico que le llegue a nuestro router por medio de un firewall. El mismo puede venir ya con el router o configurable desde la red, depende del hardware que se compre. De cualquier modo es una pieza muy importante para la seguridad de nuestra red.

La segunda es la implementación de una NAT (Network Address Translation) que renombre a las direcciones origen de nuestra red. Esto hace que las direcciones reales de nuestras computadoras no serán visibles desde fuera de la red.

Por último también implementaríamos una lista de direcciones MAC permitidas, que sería configurada en el router. Esto asegura que el tráfico que no sea de una de estas direcciones sea descartado.

2. Ejercicio 2

Vamos a querer conectarnos a un servidor web desde una PC. Al tener configurado un servidor Proxy para acceder a recursos HTTP, el pedido GET desde la computadora al navegador va a ser enviado al Proxy. Suponiendo que el Proxy está configurado a partir de su dirección IP y la PC la conoce, no es necesario hacer una consulta DNS en este caso.

Como la PC no tiene en su cache ARP la dirección MAC del Proxy, broadcastea por la red un request ARP tipo `who-has` preguntando por la direccion IP del Proxy. Este paquete le llega al Hub quien lo reenvía al Switch 1. Como este no tiene en su tabla de forwarding una entrada para el Proxy, lo broadcastea por sus demás salidas. Cuando le llega al Router1, al tener configurado ruteo estático, descartará el paquete. Al llegar al Proxy, como la IP coincide con la propia, envía un response ARP tipo `i-am` con su dirección MAC a la PC.

En este proceso, el Switch 1 aprende la ubicación de la PC y el Proxy. Al recibir el Switch 1 el paquete `response-ARP`, lo envía a la PC por su interfaz 0. Una vez que le llega a la PC, esta agrega la entrada correspondiente en su cache ARP, que queda configurada de la siguiente manera.

Cache ARP PC	
IP	MAC
IP Proxy	MAC Proxy

Luego, se le va a enviar un paquete TCP de tipo HTTP GET al Proxy desde la PC para poder acceder al recurso. Este paquete inicialmente será enviado al Hub, que a su vez lo va a enviar al Switch 1. Este se lo envía directamente al Proxy según indica su tabla de forwarding.

Una vez recibido el request HTTP en el servidor Proxy, este va a necesitar saber la dirección IP destino, por lo que va a disparar una consulta DNS para poder mapear la URL a la que nos queremos conectar con la IP del servidor web. Al tener, por enunciado, todas las resoluciones DNS en las caches locales, el Resolver automáticamente nos va a responder desde la caché la IP del servidor web, la cual es 200.1.17.4.

Luego de recibir el paquete con el pedido GET y traducir la URL a una IP, el Proxy debe resolverlo, para esto, va a enviarlo al servidor web. Como la IP destino no pertenece a su red, va a enviar el paquete IP a la interfaz correspondiente del Router 1, pero como no conoce la dirección MAC de esta interfaz envía primero un paquete request ARP tipo `who-has` preguntando por la IP de dicha interfaz. Se va a enviar el paquete a través del único puerto de salida que tiene, hacia el Switch 1. El Switch 1 lo broadcastea porque no conoce el destino, eventualmente le llega al Router 1 quien envía un response ARP tipo `i-am` al Proxy. Esta respuesta le llega al Switch 1 quien aprende la ubicación del router y reenvía la respuesta al Proxy. Una vez que este último tiene la dirección MAC del router, le envía el pedido GET con destino al servidor web. La cache ARP del servidor Proxy queda de la siguiente manera:

Cache ARP Servidor Proxy	
IP	MAC
IP IF0 ROUTER 1	MAC IF0 ROUTER 1

El Router 1 al recibir el paquete lo envía por la interfaz 1, correspondiente a la red de la IP destino. El Router 2 recibe el paquete, realiza a través de NAPT la traducción de la IP origen privada a su correspondiente IP pública y ve que la IP destino corresponde a la red de su interfaz 1, pero no conoce la dirección MAC de la misma por lo que envía por la red un request ARP tipo `who-has` preguntando por la IP del servidor web.

Asumimos que el Firewall de esta red está configurado en el Router 2 y deja pasar todos los paquetes con destino al servidor web.

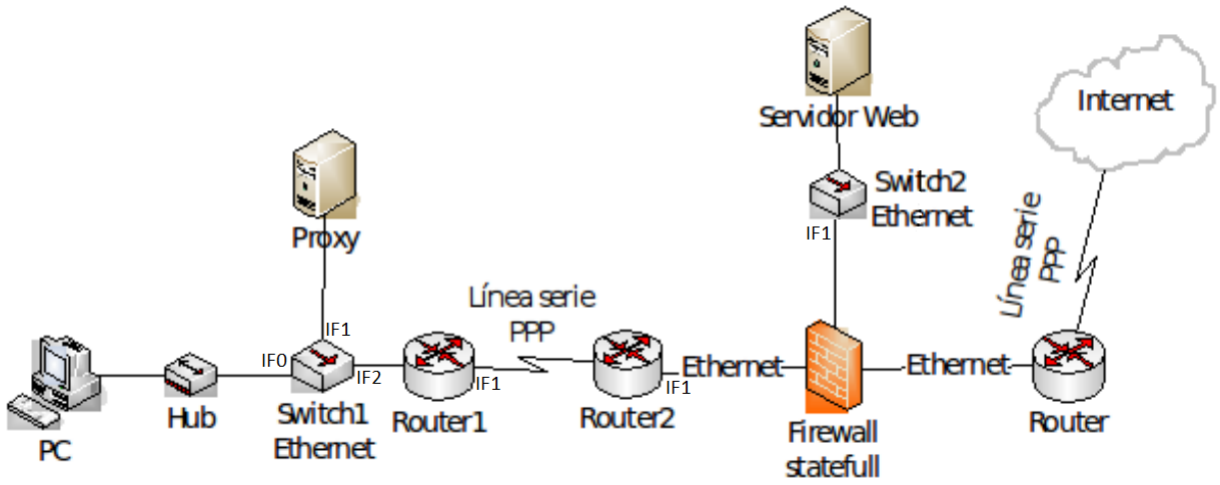

Figura 2: Estructura de la red con interfaces numeradas

Al recibirlo, el Switch 2 aprende la dirección MAC de la interfaz 1 del Router 2 y, como no conoce la dirección de destino del paquete, lo reenvía por sus demas salidas. Así el paquete le llega finalmente al servidor web quien entonces le envía al Router 2 un response ARP tipo `i-am`. Así, la cache ARP del Router 2 queda configurada como:

Cache ARP Router 2	
IP	MAC
200.1.17.4	MAC Servidor Web

Una vez que el Router 2 cuenta con la dirección MAC del servidor web, le envía el request HTTP GET al mismo, quien lo recibe a través del Switch 2. En este punto, el paquete ya llegó a destino.

Al finalizar el envío del paquete HTTP GET desde la PC al Servidor Web, las tablas de forwarding de los switches quedan configuradas de la siguiente manera:

Tabla de Forwarding Switch 1		
MAC	PUERTO	COMENTARIOS
PC MAC Address	IF 0	Aprendida cuando le llega el paquete request ARP de la PC hacia el Proxy.
PROXY MAC Address	IF 1	Aprendida cuando le llega el paquete response ARP del Proxy hacia la PC.
ROUTER 1 IF0 MAC Address	IF 2	Aprendida cuando le llega el paquete response ARP del Router hacia el Proxy.

Tabla de Forwarding Switch 2		
MAC	PUERTO	COMENTARIOS
ROUTER 2 IF1 MAC address	IF 1	Aprendida cuando le llega el paquete request ARP del Router hacia el servidor web.