UNCUYO UNIVERSIDAD NACIONAL DE CUYO | FACULTAD DE INGENIERÍA | Licenciatura en Ciencias de la Computación

Redes de Computadoras
Trabajo práctico Nº2 - 2022
Componentes y tramas en redes Ethernet y IEEE802.11. VLANs

Objetivos

Repasar los conocimientos adquiridos en clases sobre protocolos de capa de Enlace y MAC mediante simulaciones y análisis de tramas.

Metodología

Trabajo individual o grupal. 2 estudiantes por grupo máximo.
Tiempo de realización: 1 clase.

Aprobación

- Enviar la simulación que se solicita en las actividades 1 y 2 funcionando (archivos .pkt). a través de la plataforma Moodle (pregunta 7 de la actividad "Trabajo Práctico N°2 - Cuestionario y entrega archivos").
- Conteste el cuestionario que encontrará en el aula abierta (Moodle) de la cátedra. Debe responder bien todas las preguntas (el cuestionario puede intentarse todas las veces que necesite). Algunas preguntas estarán referidas a la simulación, por lo que deberá realizar primero la simulación y tenerla a mano cuando conteste el cuestionario.

Materiales necesarios

- Computadoras con acceso a Internet (provistas por la facultad de Ingeniería).
- Simulador de redes Cisco Packet Tracer (puede descargarlo sin costo). Para utilizar Cisco Packet Tracer es necesario crear una cuenta en Netacad.
    - Para crear cuenta en Netacad para utilizar Cisco Packet Tracer: ir a https://www.netacad.com/es/ , luego ir a "cursos->packet tracer>skillsforall.com/" e inscribirse a un curso (recuerde el usuario y contraseña creado, se pedirá cuanto quiera acceder a Cisco Packet Tracer)
    - Para descargar Cisco Packet Tracer (no tiene costo), acceda a su cuenta en https://www.netacad.com/es/, luego ir a "Recursos->Descargar Packet Tracer" y seleccione el sistema operativo adecuado.
- Analizador de tráfico de red Wireshark (puede descargarlo sin costo desde www.wireshark.org/download.html o los repositorios de Linux con "*sudo apt-get install wireshark"*. Fue utilizado en el trabajo práctico N°1).

Actividades

Actividad 1: Redes Ethernet, switches y hubs

Ingrese a Packet Tracer y arme la red que se muestra en la figura 2 (En el Anexo 1 encontrará un breve resumen de uso del PacketTracer). Se sugiere utilizar los nombres indicados en la figura.

- Para los switches, utilice el modelo 2950-24 (24 puertos).
- Para unir las Laptop a los switches o hubs, utilice cables del tipo Copper Straight-Through o cable directo (líneas sólidas).
- Para unir los switches o hubs entre si, utilice cables del tipo Copper Cross-Over o cable cruzado (líneas punteadas).
  (Puede ver en el Anexo 2 una explicación de la diferencia entre cables directos y cables cruzados).
- Configure las interfaces Ethernet de las computadoras como sigue (hacer doble clic sobre la computadora, luego config->Interface->Ethernet):
  - IP Configuration: Static
  - IP Address: 200.0.0.1 para la Laptop1, 200.0.0.2 para la Laptop2, 200.0.0.3 para la Laptop3, etc. Para todos, máscara de red 255.255.255.0.

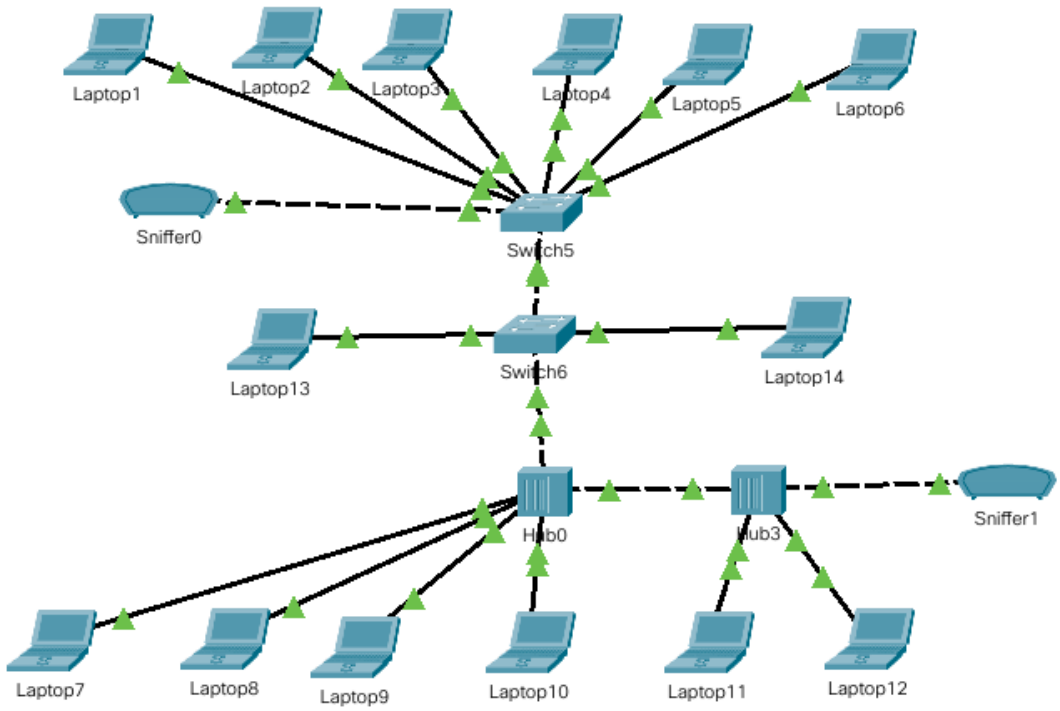


Figura 2: Red a simular en Packet Tracer

- Verifique la conectividad mediante el comando “ping”. Para ello:
    - Haga doble clic sobre la laptop desde la cual desee probar conectividad. Vaya a Desktop (escritorio)->Command Prompt (símbolo del sistema).
    - Escriba “ping x.x.x.x”, donde x.x.x.x es la laptop con la cual desea probar conectividad. Ejemplo, si desea verificar si la laptop cuya IP es 200.0.0.2 puede ver a la laptop 200.0.0.4, debe escribir “ping 200.0.0.4” desde la consola de comandos de la laptop 200.0.0.2.
    - Si recibe mensajes “Reply from” con algunos datos, significa que las computadoras “pueden verse”.
    - Si recibe mensajes indicando “Request timed out”, significa que las máquinas no pueden verse.
- Verifique si el sniffer1 (dispositivo de hardware y/o software capaz de ver y analizar la información que circula por la red) puede capturar el tráfico entre dos máquinas. Para ello:
    - Envíe repetidamente comandos ping entre las máquinas laptop7 y laptop8. Para ello, utilice el comando “ping -n 100 x.x.x.x”, donde -n 100 indica que deben enviarse 100 peticiones de eco.

    - Mientras la laptop7 y la laptop8 se comunican, verifique si el sniffer1 puede ver la comunicación. Para ello, haga doble clic en el sniffer, vaya a GUI y verifique si ve tramas ICMP (Protocolo utilizado por el comando PING). Si ve tramas ICMP, significa que el sniffer puede "ver" la comunicación (Se sugiere borrar los mensajes vistos por el sniffer antes de verificar si puede ver mensajes ICMP con el botón "Clear").
        - Nota: Verá tramas STP. Este es un protocolo de capa de enlace (STP: **S**panning **T**ree **P**rotocol o Protocolo de árbol de expansión). En una red con varios switches, STP determina rutas entre dispositivos evitando lazos cerrados (debe haber visto árboles de expansión como parte de su carrera).
- Repita para el sniffer0 (por ejemplo, verificando si el sniffer0 puede ver la comunicación entre las laptop 1 y 2).
- Utilizando el dispositivo sniffer, analice un paquete ICMP y un paquete STP. Analice como se encapsulan.
- Responda las preguntas planteadas en la plataforma Moodle relacionadas con esta actividad (se sugiere responder con la simulación corriendo).

Actividad 2: LAN virtuales (VLAN).

Divida la red implementada en dos LAN virtuales, de modo que las máquinas 1, 2, 3, 4, 5, 6, y 13 queden en una misma VLAN, y las máquinas 7, 8, 9, 10, 11, 12 y 14 queden en otra VLAN diferente. Para ello, siga los siguientes pasos:

- En cada switch, debe crear las dos redes VLAN (una ya estará creada por defecto). Para ello:
    - Haga doble clic en el switch, vaya a "VLAN Database", en el campo "VLAN number" escriba 2 (o el número que desee), y en "VLAN name" el nombre de la nueva VLAN (ejemplo: "supervision"). Importante: debe indicar el mísmo número y nombre en todos los switches.
    - En cada switch, indique a que VLAN se conectará cada puerto del switch. Para ello, en la ventana de configuración del switch, ingrese a las pestañas de cada uno de los puertos (Ethernet0/1, Ethernet0/2, etc.), seleccione el modo "Access", y en el campo VLAN, seleccione el número de VLAN para ese puerto.
        - Nota: Puede ver el número de puerto del switch al que está conectada cada computadora si en el menú option->preferences selecciona "Always Show Port Labels in Logical Workspace".

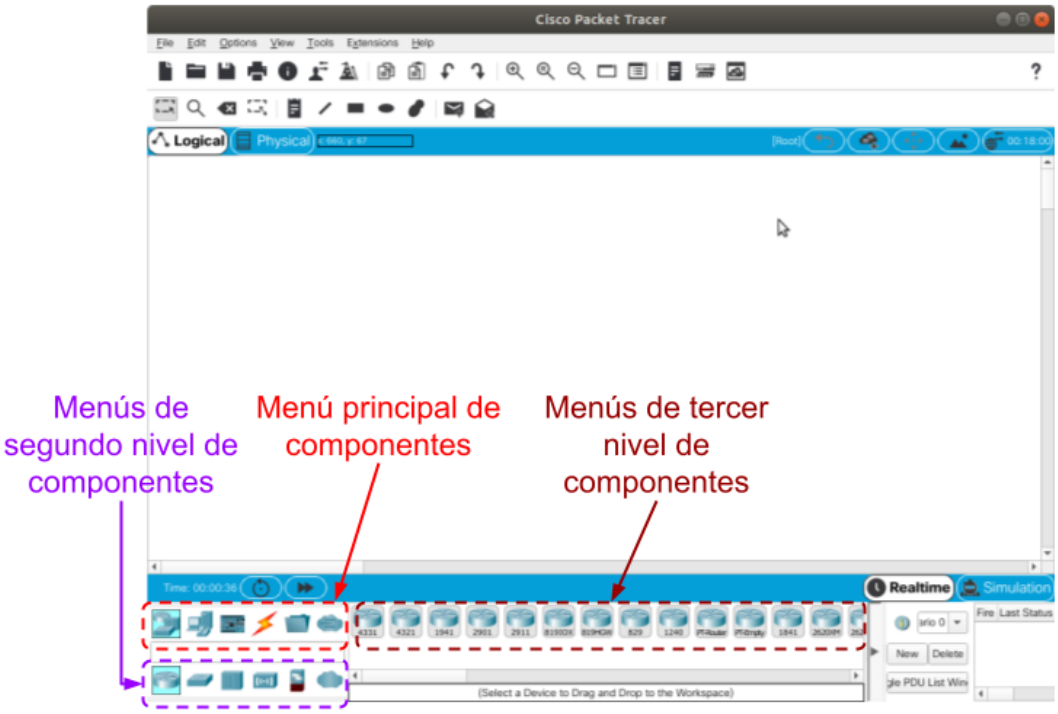
    - Si necesita conectar un dispositivo a más de dos VLAN, seleccione el modo “Trunk” en lugar de “Access” en el menú desplegable junto al menú de selección de número de VLAN.
- Verifique si las computadoras en una misma VLAN pueden comunicarse mediante el comando ping.
- Verifique si computadoras en diferentes VLAN pueden comunicarse.

Actividad 3: Colisiones

- Envíe un comando ping desde la máquina 13 a todas las máquinas de la VLAN1. Para enviar un ping a todas máquinas utilice la dirección 200.0.0.255 (la mayor de las direcciones IP de una red es la dirección de broadcast). Envíe el comando con una sola repetición para un mejor análisis de las respuestas, para ello utilice ping -n 1 200.0.0.255. Verifique si responden todas las máquinas de la VLAN1 o no.
- Envíe un comando ping desde la máquina 14 a todas las máquinas de la VLAN2. Verifique si responden todas las máquinas de la VLAN2 o no.
- Analice detalladamente como se mueven los paquetes en la red utilizando modo “simulación” (este modo permite ver paso a paso de como se comportan los paquetes). En el modo simulación, se sugiere editar filtros (Pestaña “Edit Filters”, borde inferior de la ventana de simulación) y desmarcar todos los paquetes de las tres pestañas IPv4, IPv6 y Misc, dejando solo marcados los paquetes ICMP de pestaña IPv4 (de lo contrario, verá todos los paquetes circulando por la red, lo que hará difícil de analizar).
    - Durante la simulación puede analizar cualquiera de los paquetes haciendo clic en el mismo. También puede pausar la simulación.

Anexo 1: Breve descripción de Cisco PacketTracer

PacketTracer es el simulador de equipamiento de redes de Cisco, el mayor fabricante de equipamiento de redes en la actualidad.

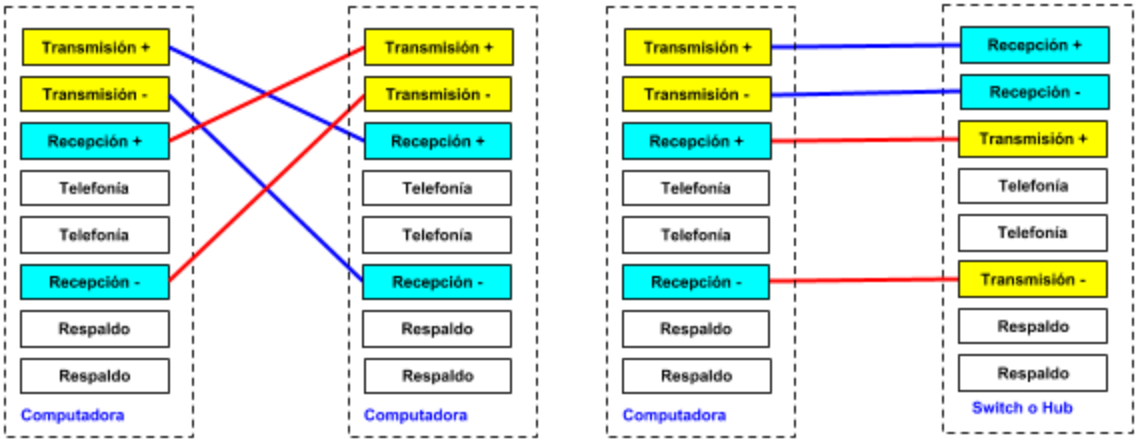


Ejemplo: Para elegir un switch, elija “Network Devices” del menú principal, luego “Switches” del menú de segundo nivel, y por último el modelo de switch en el menú de tercer nivel.

Anexo 2: Cables directos y cruzados:

La interfaz física RJ45 (conector) es el estándar empleado en redes Ethernet de par trenzado. La misma establece las características eléctricas y mecánicas del conector y la distribución de pines de la ficha.

En las primeras redes Ethernet de par trenzado, para conectar directamente dos computadoras, dos switches, dos hubs o un switch con un hub era necesario cruzar los pares trenzados del cable de modo que los pines de transmisión de un extremo queden conectados a los pines de recepción en el otro extremo, como se muestra en la figura 1. En cambio, los switches y hubs cruzaban las conexiones dentro del propio aparato, de modo que para conectar una computadora a un switch o hub, los cables debían ser directos, como se muestra en la figura 1.



(a) Cable cruzado (b) Cable directo

Figura 1: (a) Cable cruzado y (b) cable directo de Ethernet de par trenzado

A partir de la norma IEEE 802.3z o 1000Base-T (año 2000), las placas de red se fabrican de modo que conmuten internamente y automáticamente las conexiones según sea necesario, por lo que no se necesitan cables cruzados para conectar dos computadoras. Por tal motivo, actualmente un mismo cable puede utilizarse para conectar una computadora a un switch o conectar dos computadoras. Sin embargo, algunos simuladores o placas viejas pueden necesitar el uso de cables directos o cruzados.