los Modelos OSI y TCP/IP

Parte 1: Configuración Básica de la Red en Packet Tracer

Para esta parte, necesitarás abrir Cisco Packet Tracer y seguir los pasos. Como no puedo interactuar directamente con Packet Tracer, te guiaré sobre lo que deberías hacer y observar.

1.1. Diseño de la red:

Arrastra dos dispositivos PC desde la sección "End Devices" al área de trabajo. Nómbralos PC1 y PC2.

Arrastra un switch desde la sección "Network Devices" > "Switches" al área de trabajo y colócalo entre los dos PCs. Puedes usar un switch 2960.

Conecta PC1 al switch usando un cable Ethernet directo (Copper Straight-Through) desde el puerto FastEthernet0/1 del switch al puerto FastEthernet0 del PC1.

Conecta PC2 al switch de la misma manera, usando el puerto FastEthernet0/2 del switch y el puerto FastEthernet0 del PC2.

1.2. Configuración de las IPs:

PC1:

Haz clic en el icono de PC1.

Ve a la pestaña "Desktop" y luego a "IP Configuration".

Selecciona la opción "Static".

Ingresa la dirección IP: 192.168.1.2

Ingresa la máscara de subred: 255.255.255.0 (la puerta de enlace predeterminada no es necesaria para esta red simple).

Cierra la ventana de configuración.

PC2:

Haz clic en el icono de PC2.

Ve a la pestaña "Desktop" y luego a "IP Configuration".

Selecciona la opción "Static".

Ingresa la dirección IP: 192.168.1.3

Ingresa la máscara de subred: 255.255.255.0

Cierra la ventana de configuración.

1.3. Verificación de conectividad:

En PC1:

Haz clic en el icono de PC1.

Ve a la pestaña "Desktop" y luego a "Command Prompt".

Escribe el comando: ping 192.168.1.3 y presiona Enter.

Deberías ver respuestas exitosas del tipo "Reply from 192.168.1.3: bytes=32 time<1ms TTL=128". Esto indica que la comunicación entre PC1 y PC2 está funcionando correctamente.

Parte 2: Análisis del Tráfico con Packet Tracer (Modelo OSI)

2.1. Simulación del tráfico:

En PC1, abre nuevamente el "Command Prompt" y ejecuta el comando ping 192.168.1.3 varias veces para generar tráfico ICMP.

Ahora, vamos a usar la función de simulación de Packet Tracer. En la esquina inferior derecha de la ventana de Packet Tracer, cambia de "Realtime" a "Simulation".

Deberías ver un panel de simulación en la parte inferior. Si no lo ves, ve a "View" > "Simulation Panel".

En el panel de simulación, haz clic en el botón "Edit Filters".

En la ventana "Edit Filters", selecciona la pestaña "ICMP" dentro de la sección "IPv4". Esto filtrará la simulación para mostrar solo el tráfico ICMP.

Ahora, haz clic en el botón "Play" (el botón que parece un triángulo apuntando hacia la derecha) en el panel de simulación para iniciar la simulación del tráfico de ping que generaste anteriormente.

Observa cómo los paquetes viajan desde PC1 al switch y luego a PC2, y cómo regresan las respuestas. Puedes usar los botones "Step Forward" para avanzar la simulación paso a paso y ver el encabezado de cada paquete en cada dispositivo.

2.2. Análisis del tráfico a través del modelo OSI:

Mientras la simulación está en pausa o mientras revisas los eventos en el panel de simulación, haz clic en uno de los eventos de ICMP (tanto el envío como la respuesta).

En la ventana de detalles del evento, ve a la pestaña "OSI Model". Aquí podrás ver cómo el paquete ICMP se encapsula y desencapsula a través de las diferentes capas del modelo OSI en cada dispositivo (PC1, el switch y PC2).

Observa la información en cada capa:

Capa 7 (Aplicación): Aunque ICMP no es una aplicación en sí misma, conceptualmente interactúa con esta capa para la solicitud de ping.

Capa 6 (Presentación): No hay una manipulación de formato significativa para ICMP en este caso.

Capa 5 (Sesión): ICMP no establece sesiones en el sentido tradicional.

Capa 4 (Transporte): ICMP opera directamente sobre la capa de red y no utiliza protocolos de transporte como TCP o UDP.

Capa 3 (Red): Aquí verás el encabezado IP con las direcciones IP de origen (192.168.1.2) y destino (192.168.1.3). El protocolo es ICMP.

Capa 2 (Enlace de Datos): Aquí verás el encabezado de la trama Ethernet con las direcciones MAC de origen y destino de las interfaces involucradas (la NIC de la PC y la interfaz del switch).

Capa 1 (Física): Esta capa representa la transmisión de los bits a través del medio físico (el cable Ethernet).

2.3. Captura de un paquete:

Mientras la simulación está activa y los pings están en curso, haz clic en el icono de un sobre que representa un paquete ICMP mientras pasa por un dispositivo (por ejemplo, entre PC1 y el switch).

En la ventana de detalles del evento que aparece, ve a la pestaña "OSI Model".

Completa la siguiente tabla con la información que observaste:

| No. de Paquete | Protocolo | Capa OSI | Fuente IP | Destino IP | Descripción |
|---|---|---|---|---|---|
| 1 | ICMP | 3 (Red) | 192.168.1.2 | 192.168.1.3 | Ping entre PC1 y PC2 |

Parte 3: Modelo TCP/IP en Packet Tracer

3.1. Comparación de capas entre los modelos OSI y TCP/IP:

El modelo TCP/IP tiene una estructura de cuatro capas que se corresponden con las siete capas del modelo OSI de la siguiente manera:

Capa de Aplicación (TCP/IP): Combina las capas de Aplicación, Presentación y Sesión del modelo OSI. Protocolos comunes en esta capa incluyen HTTP, FTP, SMTP, DNS, etc.

Capa de Transporte (TCP/IP): Se corresponde directamente con la Capa de Transporte del modelo OSI. Los protocolos principales son TCP (orientado a la conexión, confiable) y UDP (sin conexión, no confiable).

Capa de Internet (TCP/IP): Se corresponde con la Capa de Red del modelo OSI. El protocolo principal es IP (Protocolo de Internet), junto con protocolos de enrutamiento como RIP y OSPF, y protocolos de control como ICMP.

Capa de Acceso a la Red (TCP/IP): Combina las capas de Enlace de Datos y Física del modelo OSI. Incluye tecnologías como Ethernet, Wi-Fi, y los protocolos de la capa MAC y la capa física.

3.2. Verificación de la funcionalidad del modelo TCP/IP:

Para observar protocolos de la capa de transporte TCP y UDP, puedes generar diferentes tipos de tráfico en Packet Tracer.

Tráfico TCP (HTTP):

Agrega un servidor al diseño de tu red (desde "End Devices"). Conéctalo al switch.

Configura una dirección IP para el servidor (por ejemplo, 192.168.1.4 con máscara 255.255.255.0).

En PC1, abre un navegador web (desde la pestaña "Desktop" > "Web Browser") e intenta acceder a la dirección IP del servidor (por ejemplo, http://192.168.1.4). Esto generará tráfico HTTP, que utiliza TCP en la capa de transporte.

Vuelve al modo de simulación y filtra por "HTTP" y "TCP". Observa el flujo de paquetes y los detalles en la pestaña "OSI Model", prestando atención a la capa de transporte (Capa 4 en OSI, Capa de Transporte en TCP/IP). Verás los segmentos TCP con números de puerto de origen y destino, y los flags de control (SYN, ACK, FIN, etc.).

Tráfico UDP (DNS):

Configura un servidor DNS en tu red (puedes usar el mismo servidor o agregar uno nuevo). Configura su dirección IP y habilita el servicio DNS.

En la configuración IP de PC1, configura el servidor DNS con la dirección IP del servidor DNS.

Desde el "Command Prompt" de PC1, ejecuta el comando nslookup google.com. Esto generará una consulta DNS, que utiliza UDP en la capa de transporte.

En el modo de simulación, filtra por "DNS" y "UDP". Observa los datagramas UDP que se envían al servidor DNS y la respuesta que regresa. Examina los detalles en la capa de transporte (Capa 4 OSI, Capa de Transporte TCP/IP) y verás los puertos de origen y destino (el puerto 53 es común para DNS).

Parte 4: Evaluación de Conocimientos

Preguntas de repaso:

¿Qué dispositivos operan en la capa de enlace de datos en la simulación?

En esta simulación, los dispositivos que operan principalmente en la capa de enlace de datos (Capa 2 del modelo OSI) son las tarjetas de interfaz de red (NICs) de los PCs y las interfaces del switch. El switch utiliza las direcciones MAC para reenviar las tramas dentro de la misma red local.

¿Qué protocolos de la capa de transporte observaste en el tráfico?

Observaste el protocolo ICMP, que aunque opera directamente sobre la capa de red (Capa 3 OSI), es fundamental para las pruebas de conectividad. Al generar tráfico HTTP, observaste el protocolo TCP. Al generar tráfico DNS, observaste el protocolo UDP.

¿Cómo se dividen las capas de los modelos OSI y TCP/IP al analizar un paquete ICMP?

Al analizar un paquete ICMP:

Modelo OSI: El paquete ICMP se originaría conceptualmente en la Capa de Aplicación (Capa 7), aunque es parte integral de la Capa de Red (Capa 3). Luego pasa por la Capa de Enlace de Datos (Capa 2) donde se agrega el encabezado de la trama Ethernet con las direcciones MAC, y finalmente a la Capa Física (Capa 1) para la transmisión. Al recibirlo, el proceso se invierte.

Modelo TCP/IP: El mensaje ICMP se considera parte de la Capa de Internet (Capa 3 del modelo OSI). Al enviarse, se encapsula en la Capa de Acceso a la Red (que combina la Capa de Enlace de Datos y Física del modelo OSI) para su transmisión.

Completa el laboratorio diseñando una red de 10 computadores y realice el mismo procedimiento de cada computador con todos:

Para esta parte, necesitarás expandir tu red en Packet Tracer:

Diseño de la red de 10 PCs:

Arrastra 10 PCs al área de trabajo.

Arrastra un switch más grande (por ejemplo, un switch de 24 puertos como el 2960-24TT) al centro.

Conecta cada PC a un puerto diferente del switch utilizando cables Ethernet directos.

Configuración de las IPs:

Asigna direcciones IP secuenciales a cada PC dentro de la misma subred (por ejemplo, 192.168.1.5 a 192.168.1.14, con máscara 255.255.255.0).

Verificación de conectividad:

Desde cada PC, haz ping a las direcciones IP de todos los demás PCs para verificar la conectividad completa. Por ejemplo, desde PC5, harías ping a 192.168.1.6, 192.168.1.7, ..., 192.168.1.14.

Análisis del tráfico:

Repite el proceso de simulación y captura de paquetes (como en la Parte 2) para el tráfico ICMP generado entre algunos pares de PCs en esta red más grande. Observa cómo el switch reenvía las tramas basándose en las direcciones MAC.

5. Lista de Verificación Ejemplo:

Revisar en la academia cisco los conceptos. (Asegúrate de haber revisado los materiales relevantes en Cisco Networking Academy sobre los modelos OSI y TCP/IP).

Subir un documento pdf al repositorio GitHub con las actividades realizadas. (Este documento debe incluir capturas de pantalla de tu topología en Packet Tracer, las configuraciones de IP, los resultados de los pings, la tabla de análisis del tráfico ICMP y tus respuestas a las preguntas de repaso).