

TRABAJO PRÁCTICO

Explorando los Modelos OSI y TCP/IP

Alumno: Ignacio Figueroa

Tecnicatura Universitaria en Programación – UTN

Materia: AySO

Comisión: 7

Objetivos

- Comprender las diferencias entre los modelos OSI y TCP/IP.
- Configurar una red básica en Packet Tracer (PT).
- Verificar el funcionamiento de los servicios DHCP, DNS y HTTP en una red.

Consignas

Parte 1: Configuración de la Red

1. Diseño de la red: Crea una topología en Packet Tracer con los siguientes elementos:
 - Una computadora (PC).
 - Un switch.
 - Un servidor DHCP.
 - Un servidor HTTP.
 - Un servidor DNS.
2. Configuración de dispositivos:
 - Configura el servidor DHCP:
 - Activa el servicio DHCP.
 - Default Gateway: 192.168.1.1.
 - DNS Server: 192.168.1.2.
 - Inicio de IPs: 192.168.1.100.
 - Configura el servidor DNS:
 - IP: 192.168.1.2.
 - Entrada DNS:
 1. Nombre: ejemplo.com.
 2. Dirección: 192.168.1.3 (IP del servidor HTTP).
 - Configura el servidor HTTP:
 - IP: 192.168.1.3.
 - Asegúrate de que el servicio HTTP esté habilitado.
 - Configura el gateway en la computadora para obtener direcciones IP automáticamente (DHCP).

Parte 2: Verificación de la Red

1. Pruebas iniciales:

- Realiza un ping desde la computadora hacia:
 - El servidor DHCP (192.168.1.1).
 - El servidor DNS (192.168.1.2). • El servidor HTTP (192.168.1.3).

2. Prueba del DNS:

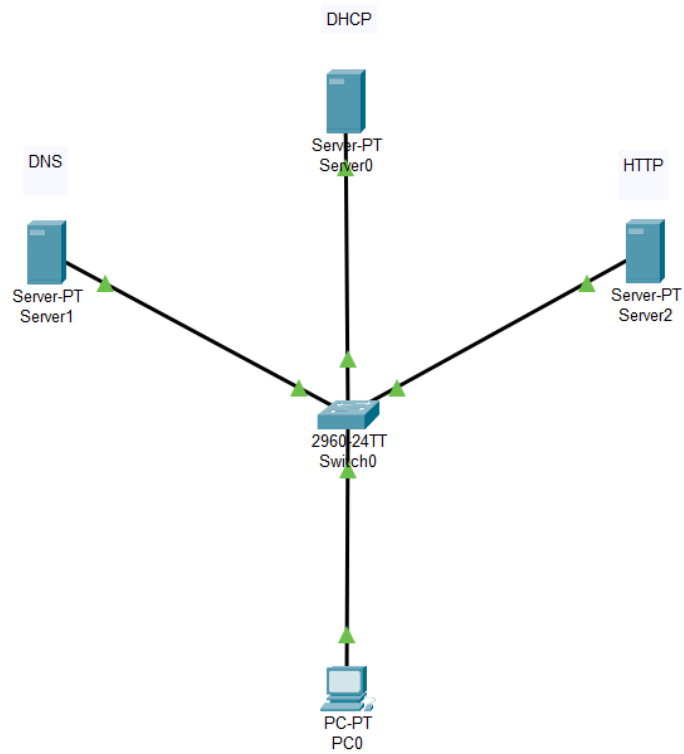
- Abre el navegador en la computadora e ingresa el nombre de dominio configurado (ejemplo.com).
- Verifica que se cargue la página del servidor HTTP.

3. Modo Simulation:

- Observa el flujo de paquetes en las diferentes capas del modelo OSI:
 - Capa 2: Verifica el uso de direcciones MAC.
 - Capa 3: Verifica las direcciones IP.
 - Capa 4: Observa el uso de TCP (HTTP) y UDP (DNS).
 - Capa 7: Verifica los servicios DNS y HTTP.

Desarrollo

Diseño de redes



Configuración del Server0 (DHCP)

Server0

Physical Config **Services** Desktop Programming Attributes

SERVICES

HTTP

DHCP

DHCPv6

TFTP

DNS

SYSLOG

AAA

NTP

EMAIL

FTP

IoT

VM Management

Radius EAP

DHCP

Interface

FastEthernet0

Service

☒ On

☐ Off

Pool Name

RedLocal

Default Gateway

192.168.1.1

DNS Server

192.168.1.2

Start IP Address :

192

168

1

100

Subnet Mask:

255

255

255

0

Maximum Number of Users :

156

TFTP Server:

0.0.0.0

WLC Address:

0.0.0.0

Add

Save

Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
RedLocal	192.168.1.1	192.168.1.2	192.168.1....	255.255.2...	156	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	192.168.1.0	255.255.2...	512	0.0.0.0	0.0.0.0

☐ Top

Configuración del Server2 (DNS)

Server2

Physical
Config
Services
Desktop
Programming
Attributes

SERVICES

HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP

DNS

DNS Service
☒ On
☐ Off

Resource Records
Name
Type
A Record

Address

Add
Save
Remove

No.	Name	Type	Detail
0	ejemplo.com	A Record	192.168.1.3

DNS Cache

☐ Top

Configuración del Server1 (HTTP)

Server1

Physical
Config
Services
Desktop
Programming
Attributes

GLOBAL

Settings

Algorithm Settings

INTERFACE

FastEthernet0

FastEthernet0

Port Status
Bandwidth
Duplex
MAC Address

☒ On
☐ 100 Mbps
☐ 10 Mbps
☒ Auto

☐ Half Duplex
☒ Full Duplex
☒ Auto

00E0.A305.D2AC

IP Configuration

☐ DHCP
☒ Static

IPv4 Address

192.168.1.3

Subnet Mask

255.255.255.0

IPv6 Configuration

☐ Automatic
☒ Static

IPv6 Address

Link Local Address:

FE80::2E0:A3FF:FE05:D2AC

☐ Top

Configuración de PC0

PC0

Physical Config Desktop Programming Attributes

IP Configuration X

Interface FastEthernet0

IP Configuration

☒ DHCP
 ☐ Static
 DHCP request successful.

IPv4 Address 192.168.1.4

Subnet Mask 255.255.255.0

Default Gateway 0.0.0.0

DNS Server 0.0.0.0

IPv6 Configuration

☐ Automatic
 ☒ Static

IPv6 Address /

Link Local Address FE80::202:17FF:FE60:1E8

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

Authentication MD5

Username

Password

☐ Top

Verificación de Red

PC0

Physical
Config
Desktop
Programming
Attributes

Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time=10ms TTL=128

Ping statistics for 192.168.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 10ms, Average = 2ms

C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.3:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>

☐ Top

Preguntas de Análisis

- A. ¿Cuál es la función de las capas 2 y 3 del modelo OSI en esta red? ¿A qué capas del modelo TCP/IP corresponden?
- B. ¿Por qué es importante el protocolo TCP para el servidor HTTP y UDP para el servidor DNS?
- C. ¿Qué sucede si el servidor DNS no está correctamente configurado?

- A. La capa 2 del modelo OSI (Capa de enlace de datos) se encarga de la comunicación y el control entre dispositivos dentro de la misma red local. La capa 3 (Capa de red) es responsable de enrutar los paquetes de datos entre diferentes redes utilizando direcciones IP. En el modelo TCP/IP, la capa 2 corresponde a la capa de acceso a la red, mientras que la capa 3 equivale a la capa de Internet.
- B. El protocolo TCP es fundamental para el servidor HTTP porque asegura que los datos se transmitan de forma fiable, ordenada y sin pérdidas, lo cual es clave para la correcta carga de páginas web. Por otro lado, el protocolo UDP es ideal para el servidor DNS porque permite enviar consultas y recibir respuestas rápidas sin establecer una conexión previa, lo que optimiza el tiempo en la resolución de nombres.
- C. Si el servidor DNS no está correctamente configurado, los dispositivos no podrán traducir nombres de dominio en direcciones IP, lo que impide que los usuarios accedan a los sitios web usando sus nombres habituales, causando fallos en la navegación y en la comunidad con otros servicios en Internet.