Redes de Computadora

Sexto Semestre ISC

JOSE ARTURO BUSTAMANTE LAZCANO

Contenido

[Introducción 2](#_Toc159916633)

[Orígenes y evolución. 4](#_Toc159916634)

[Conceptos básicos de redes 6](#_Toc159916635)

[Direccionamiento IP 8](#_Toc159916636)

[Practica 1 Segmento de red 192.168.0.0/24 9](#_Toc159916637)

[Clasificación de redes 12](#_Toc159916638)

# Introducción

=====================================

Las redes de computadoras son una parte fundamental en la tecnología moderna, ya que permiten conectar dispositivos electrónicos y facilitan la comunicación entre ellos. En este capítulo, exploraremos los

conceptos básicos de las redes de computadoras, incluyendo sus componentes, tipos de redes y cómo funcionan.

Componente Básico: el Nodo

-------------------------

Un nodo es cualquier dispositivo que forma parte de una red de computadoras. Los nodos pueden ser ordenadores personales, servidores, routers, switches o cualquier otro dispositivo conectado a la red.

Cada nodo tiene un conjunto de características clave, como la dirección IP, el puerto Ethernet y la capacidad de transmitir y recibir datos.

Tipos de Redes

--------------

Existen dos tipos principales de redes de computadoras:

### Redes Locales

Las redes locales son aquellas que conectan dispositivos en un mismo lugar, como una oficina o una casa. Estas redes suelen utilizar tecnologías como Ethernet o Wi-Fi para permitir la comunicación entre

los dispositivos.

### Redes de Área Amplia

Las redes de área amplia son aquellas que conectan dispositivos en diferentes lugares, como ciudades o países. Estas redes suelen utilizar tecnologías como Internet o redes Wi-Fi para permitir la comunicación entre los dispositivos.

Comunicación en Redes

-------------------

La comunicación en redes de computadoras se basa en el uso de protocolos de comunicación, que son setas de lenguaje que describen cómo se envían y se reciben datos en la red. Los protocolos más comunes

incluyen TCP/IP, HTTP, FTP, SMTP y DNS.

Protección de Redes

------------------

La protección de redes es importante para garantizar la seguridad de los datos transmitidos a través de la red. Algunos de los métodos utilizados para proteger las redes incluyen el uso de firewall, Virtual Private Network (VPN) y cifrado de red.

Conclusión

----------

En resumen, las redes de computadoras son un conjunto de dispositivos conectados para facilitar la comunicación entre ellos. Los nodos son los dispositivos que forman parte de la red, mientras que los

protocolos de comunicación describen cómo se envían y se reciben datos en la red. La protección de redes es importante para garantizar la seguridad de los datos transmitidos a través de la red.

## Orígenes y evolución.

Las redes han experimentado una evolución significativa a lo largo del tiempo, desde sus primeras manifestaciones hasta las complejas infraestructuras interconectadas que conocemos hoy en día. Aquí hay un breve resumen del origen y la evolución de las redes:

Década de 1960: ARPANET y los inicios de Internet:

El origen de las redes modernas se remonta a ARPANET (Advanced Research Projects Agency Network), que fue desarrollada por el Departamento de Defensa de los Estados Unidos en la década de 1960.

ARPANET fue la primera red en utilizar el protocolo de conmutación de paquetes, que dividía los datos en paquetes para facilitar la transmisión.

Década de 1970: TCP/IP y la expansión de Internet:

Se introdujo el protocolo TCP/IP (Transmission Control Protocol/Internet Protocol), que se convirtió en el estándar para la comunicación en red.

La investigación y el desarrollo de las redes se extendieron a nivel internacional, y surgieron diversas redes independientes que eventualmente se conectarían para formar la base de lo que conocemos como Internet.

Década de 1980: Redes locales (LAN) y Redes de Área Extensa (WAN):

Se popularizaron las redes locales (LAN) para interconectar dispositivos en un área geográfica limitada, como una oficina.

Las Redes de Área Extensa (WAN) permitieron la conexión de redes locales a través de distancias mayores.

Década de 1990: La explosión de Internet y la World Wide Web:

Internet se volvió accesible para el público en general, y la World Wide Web (WWW) permitió la creación y distribución de información de manera más fácil y rápida.

Se desarrollaron estándares como HTTP (Hypertext Transfer Protocol) y HTML (Hypertext Markup Language) para facilitar la creación y visualización de contenido web.

Década de 2000: Redes inalámbricas y móviles:

El auge de las tecnologías inalámbricas, como Wi-Fi y redes móviles (3G, 4G), permitió una mayor movilidad y acceso a Internet desde dispositivos móviles.

Década de 2010 hasta la actualidad: Internet de las cosas (IoT) y 5G:

La proliferación de dispositivos conectados en el Internet de las cosas (IoT) ha llevado a una mayor interconexión de objetos cotidianos.

La implementación de la tecnología 5G ha proporcionado velocidades de conexión aún más rápidas y mayor capacidad para manejar la creciente cantidad de dispositivos conectados.

La evolución de las redes sigue en curso, con desarrollos en áreas como la inteligencia artificial, la computación en la nube y la seguridad de la información que continúan influyendo en su desarrollo.

# Conceptos básicos de redes

Las redes son sistemas de comunicación que conectan diferentes dispositivos electrónicos entre sí con el fin de compartir recursos, datos y servicios. Aquí tienes algunos conceptos básicos relacionados con las redes:

Nodos: Son los dispositivos conectados en una red, como computadoras, impresoras, routers, switches, entre otros.

Enlaces: Son las conexiones físicas o lógicas entre los nodos de una red. Pueden ser alámbricos, como cables de Ethernet, o inalámbricos, como conexiones WiFi.

Protocolo: Es un conjunto de reglas y estándares que establecen cómo los dispositivos en una red se comunican entre sí. Ejemplos de protocolos comunes son TCP/IP (Transmission Control Protocol/Internet Protocol) y HTTP (Hypertext Transfer Protocol).

Topología de red: Es la estructura física o lógica de una red, que define cómo están interconectados los nodos y los enlaces. Algunas topologías comunes son bus, anillo, estrella y malla.

Dirección IP: Es un identificador único asignado a cada dispositivo en una red que utiliza el protocolo de Internet para comunicarse. Las direcciones IP pueden ser IPv4 (por ejemplo, 192.168.1.1) o IPv6 (por ejemplo, 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

Dirección MAC: Es un identificador único grabado en la tarjeta de red de un dispositivo, que se utiliza para identificarlo en una red local.

Router: Es un dispositivo que interconecta redes informáticas y dirige el tráfico de datos entre ellas. Los routers también pueden proporcionar funciones de firewall, NAT (Network Address Translation) y otros servicios.

Switch: Es un dispositivo de red que conecta múltiples dispositivos en una red local y dirige el tráfico de datos entre ellos. Los switches operan en la capa de enlace de datos del modelo OSI (Open Systems Interconnection).

Firewall: Es un sistema de seguridad que controla y filtra el tráfico de red basado en reglas predefinidas, con el fin de proteger una red de amenazas externas e internas.

Protocolo de enrutamiento: Es un protocolo utilizado por los routers para determinar la mejor ruta para enviar datos a su destino en una red.

Estos son solo algunos conceptos básicos de redes, pero hay muchos más términos y tecnologías relacionadas con este campo.

# Direccionamiento IP

¿Qué es una dirección IP?

Una dirección IP (del inglés, Internet Protocol) es una etiqueta numérica que identifica de manera única a un dispositivo conectado a una red que utiliza el protocolo IP. Es como la dirección postal de tu casa, pero para el mundo digital.

Formato de una dirección IP:

Las direcciones IP se expresan como un conjunto de cuatro números decimales separados por puntos, como por ejemplo: 192.168.1.38. Cada número puede variar entre 0 y 255, lo que da un total de 4.294.967.296 direcciones IP posibles.

Tipos de direcciones IP:

Estáticas: Son direcciones fijas que se asignan manualmente a un dispositivo. Se utilizan para servidores, impresoras y otros dispositivos que necesitan ser siempre accesibles en la red.

Dinámicas: Son direcciones que se asignan automáticamente a un dispositivo por un servidor DHCP (Dynamic Host Configuration Protocol) cada vez que se conecta a la red. Se utilizan para la mayoría de los dispositivos domésticos, como laptops, smartphones y tablets.

Funciones de la dirección IP:

Identificación: Permite identificar de forma única a un dispositivo en la red.

Ubicación: Indica la red a la que pertenece un dispositivo.

Enrutamiento: Permite que los datos se envíen al dispositivo correcto en la red.

Clases de direcciones IP:

Las direcciones IP se dividen en diferentes clases según el primer número del conjunto:

Clase A: Se utilizan para redes grandes, como las de empresas o universidades.

Clase B: Se utilizan para redes medianas, como las de oficinas o escuelas.

Clase C: Se utilizan para redes pequeñas, como las de hogares o pequeñas empresas.

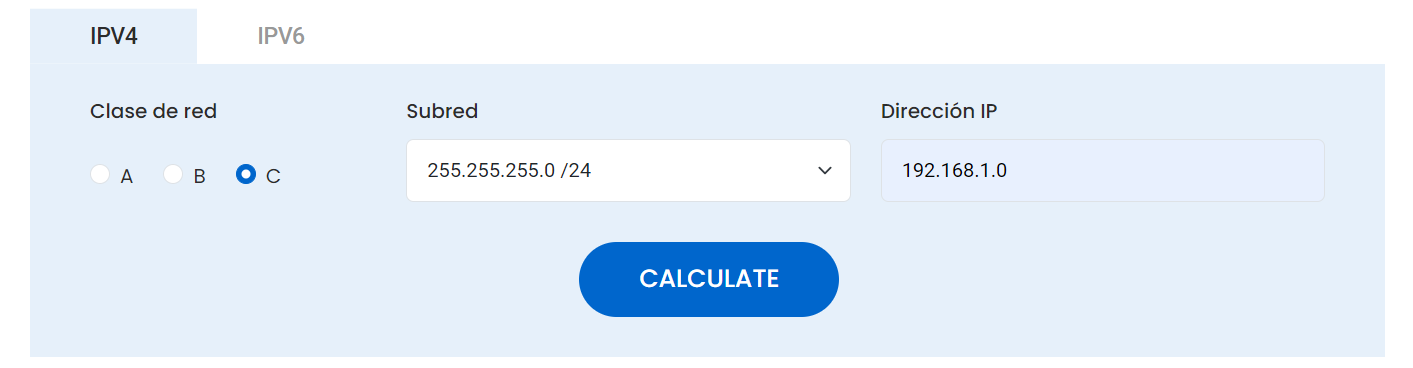
Subredes:

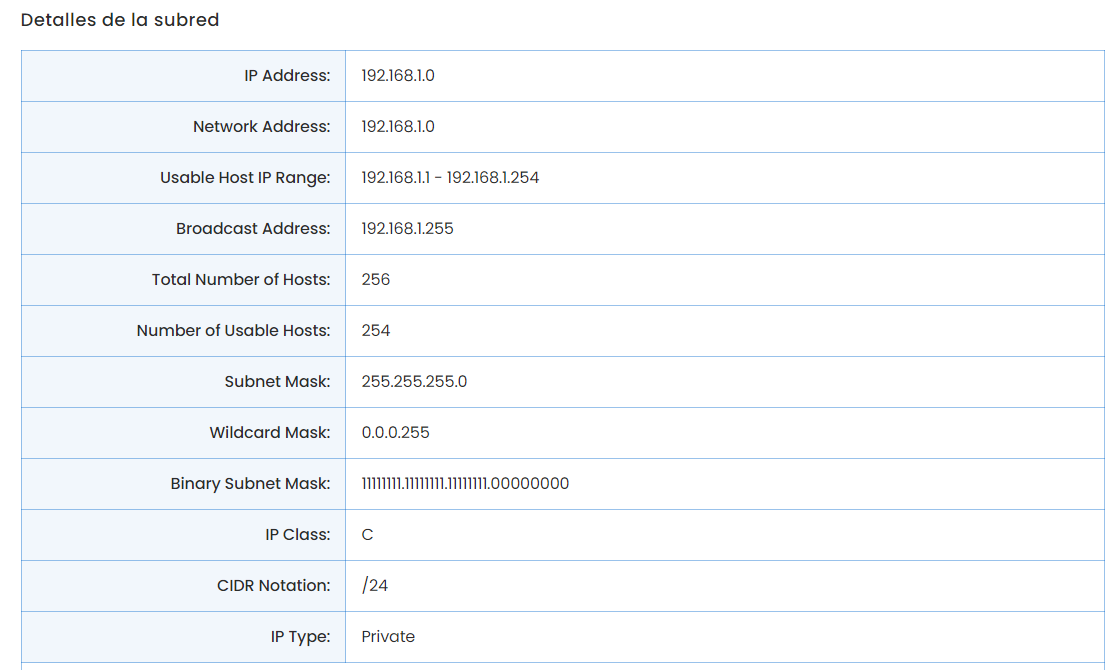
Las redes se pueden dividir en subredes para mejorar la eficiencia del tráfico y la seguridad. Una subred es un grupo de dispositivos dentro de una red que comparten una parte de la dirección IP.

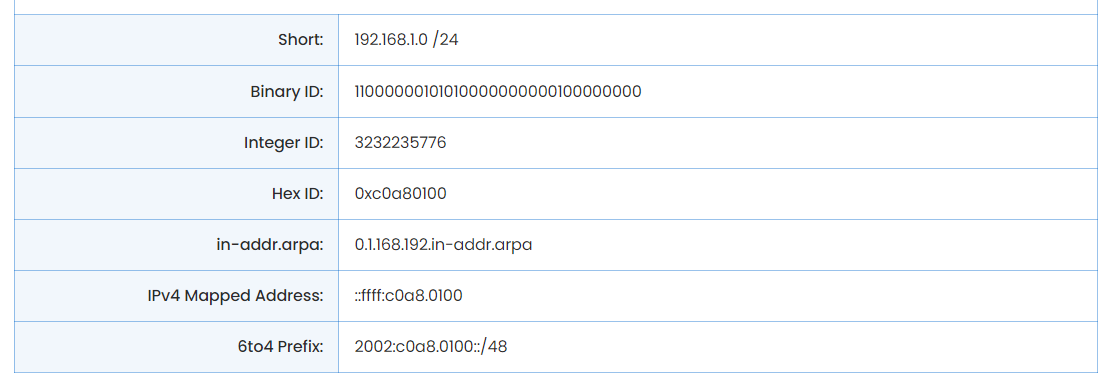
## Practica 1 Segmento de red 192.168.0.0/24

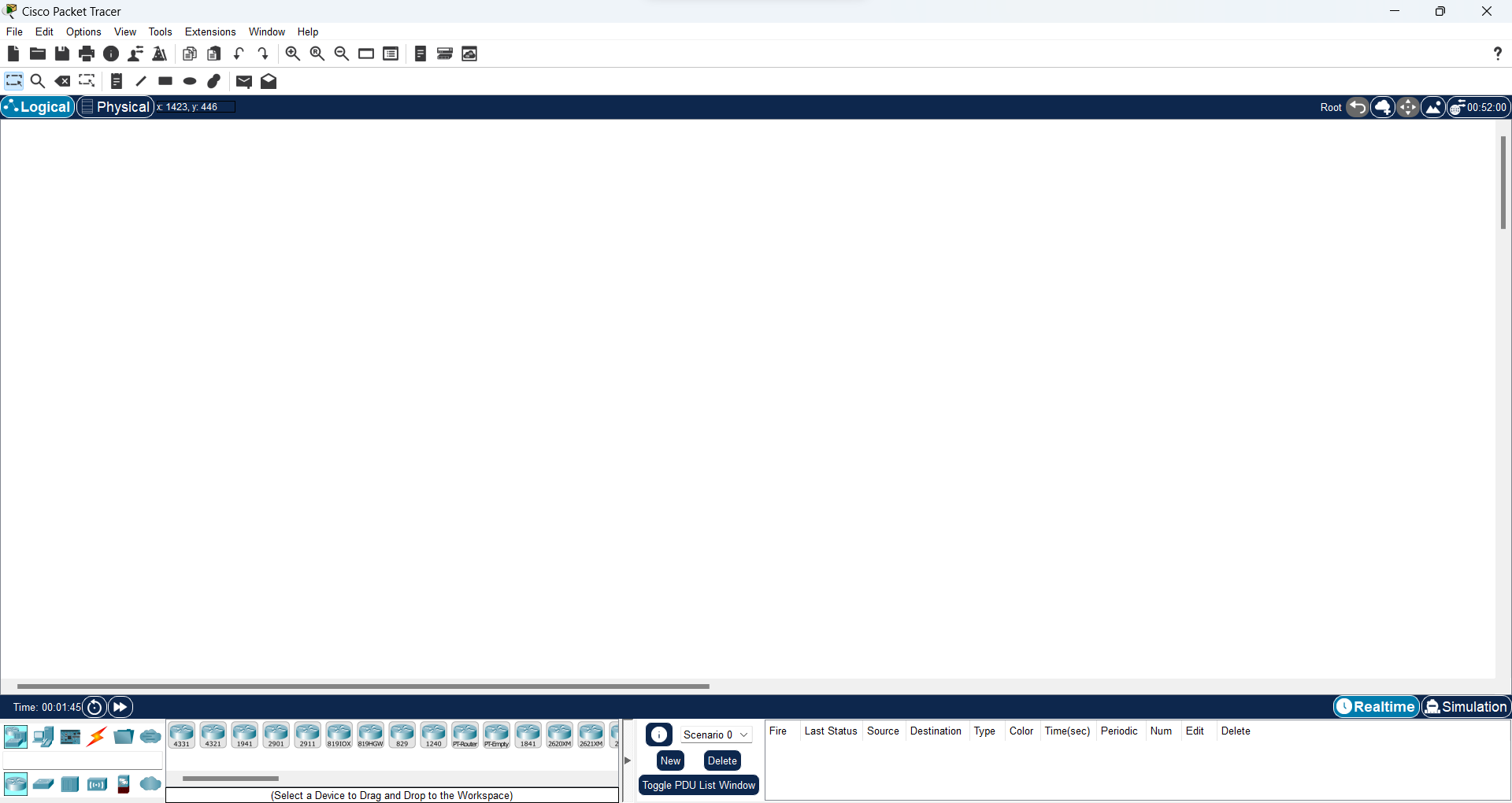
Herramienta <https://www.iptp.net/es_ES/iptp-tools/ip-calculator/>

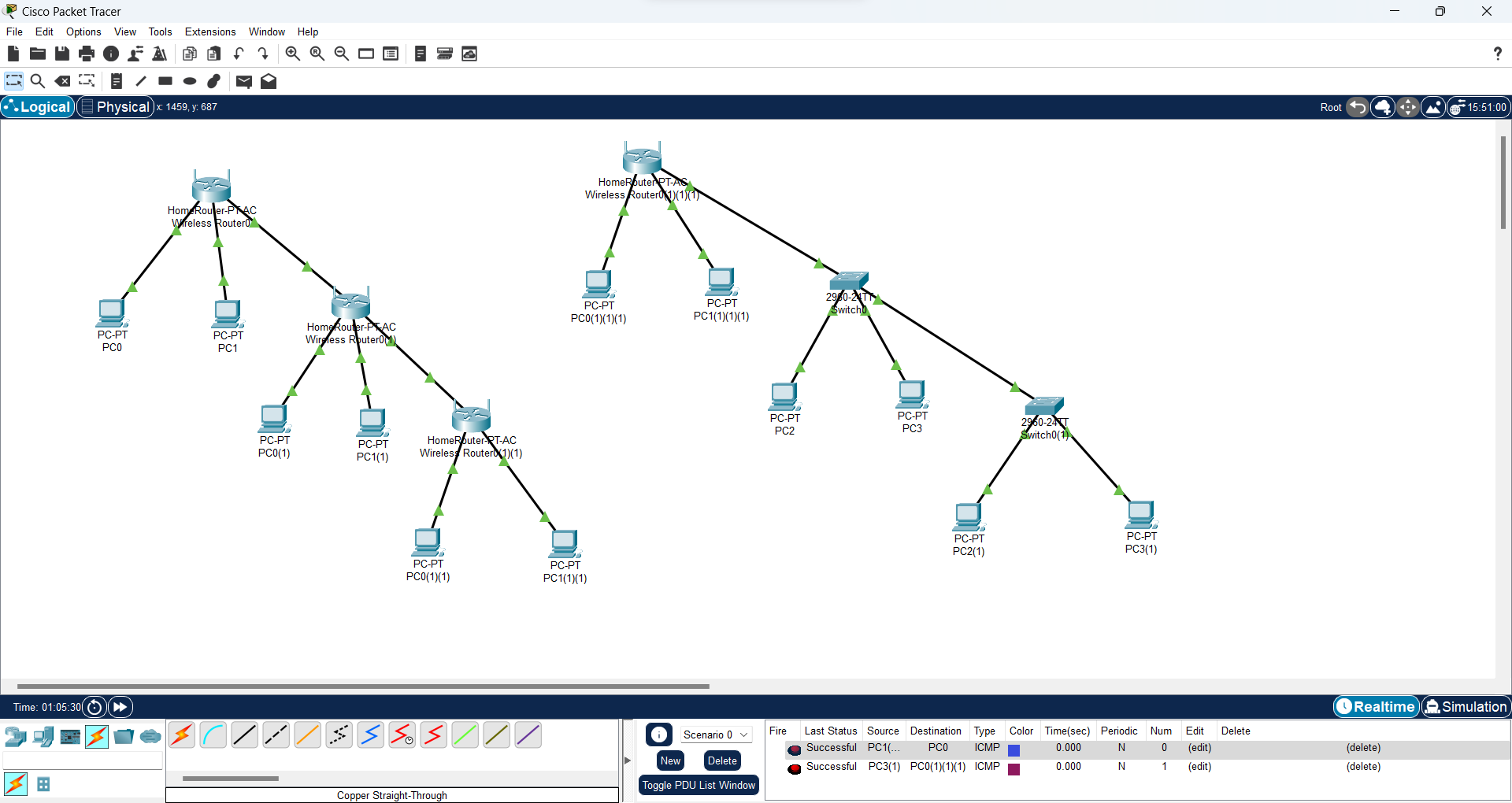
Calculo 1

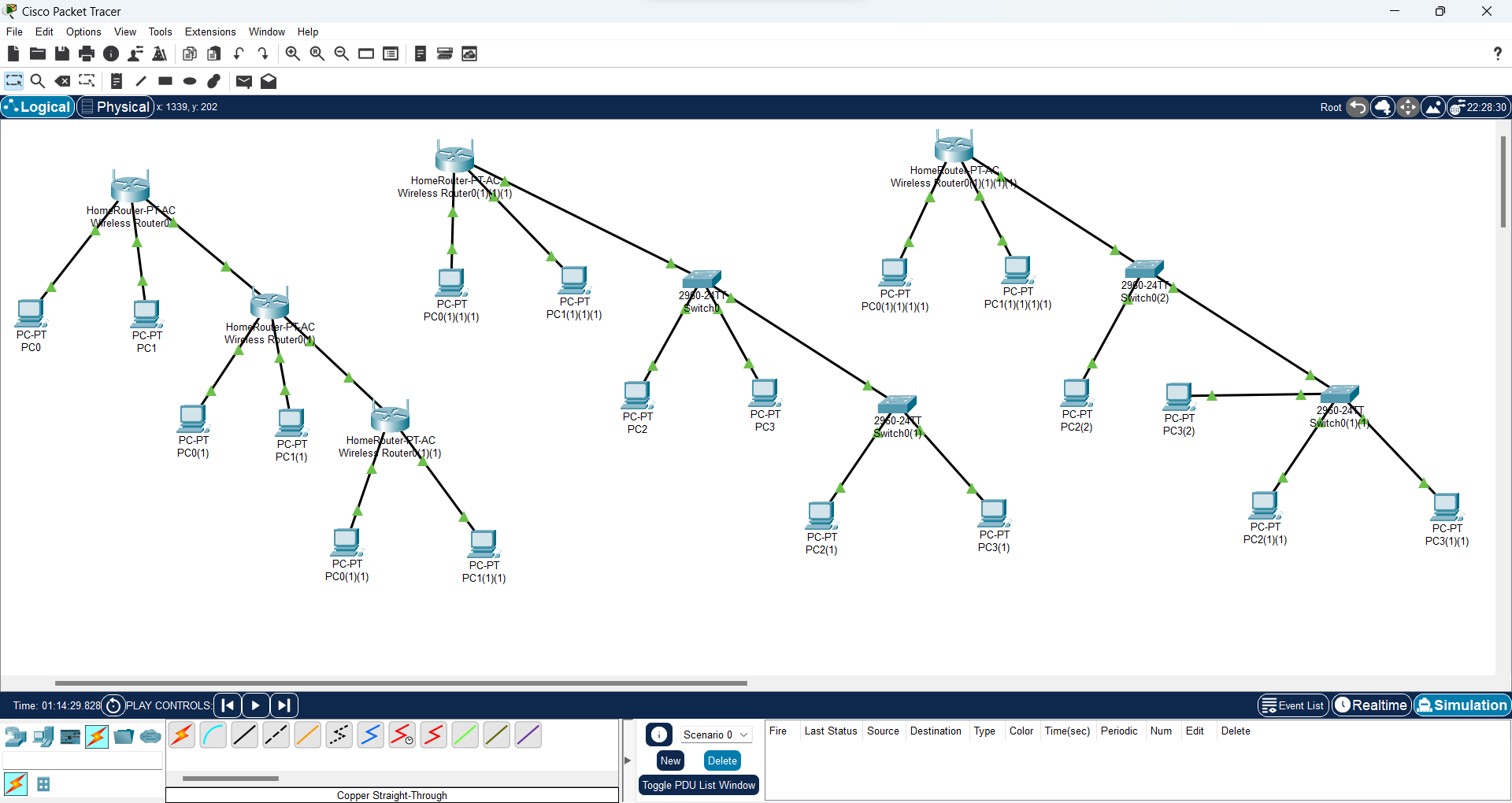












# Clasificación de redes

Las redes informáticas se pueden clasificar según varios criterios, como el tamaño, el alcance, la topología y el medio de transmisión.

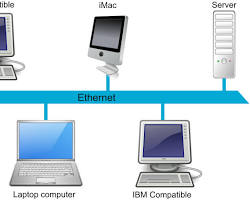
**Por tamaño:**

* **Red de área personal (PAN)**: una red que abarca un área pequeña, como el espacio alrededor de una persona. Los dispositivos PAN se comunican entre sí mediante tecnologías inalámbricas como Bluetooth e infrarrojos.

[Se abre en una ventana nueva[](https://redesinformaticas.org/red-pan/)redesinformaticas.org](https://redesinformaticas.org/red-pan/)

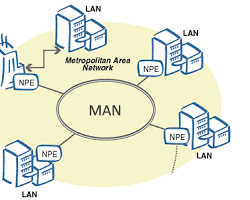
Red de área personal (PAN)

* **Red de área local (LAN )**: una red que abarca un área limitada, como una casa, un edificio o un campus. Las redes LAN se utilizan normalmente para conectar computadoras, impresoras y otros dispositivos. Los dispositivos LAN se comunican entre sí mediante cables o tecnologías inalámbricas como Wi-Fi.

[Se abre en una ventana nueva[](https://es.wikipedia.org/wiki/Red_de_%C3%A1rea_local)es.wikipedia.org](https://es.wikipedia.org/wiki/Red_de_%C3%A1rea_local)

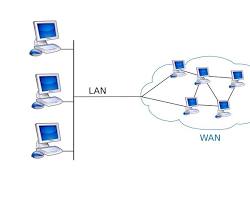
Red de área local (LAN)

* **Red de área metropolitana (MAN)**: una red que abarca un área más grande que una LAN, como una ciudad o un área metropolitana. Las MAN se utilizan normalmente para conectar redes LAN entre sí. Los dispositivos MAN se comunican entre sí mediante cables de fibra óptica u otros medios de alta velocidad.

[Se abre en una ventana nueva[](https://es.wikipedia.org/wiki/Red_de_%C3%A1rea_metropolitana)es.wikipedia.org](https://es.wikipedia.org/wiki/Red_de_%C3%A1rea_metropolitana)

Red de área metropolitana (MAN)

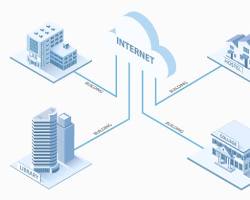
* **Red de área amplia (WAN)**: una red que abarca un área grande, como un país o un continente. Las WAN se utilizan normalmente para conectar redes MAN entre sí. Los dispositivos WAN se comunican entre sí mediante cables de fibra óptica, satélites u otros medios de comunicación de larga distancia.

[Se abre en una ventana nueva[](https://es.wikipedia.org/wiki/Red_de_%C3%A1rea_amplia)es.wikipedia.org](https://es.wikipedia.org/wiki/Red_de_%C3%A1rea_amplia)

Red de área amplia (WAN)

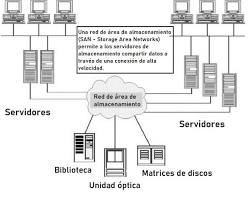
**Por alcance:**

* **Campus Area Network (CAN)**: una red que abarca un área más grande que una LAN pero más pequeña que una MAN. Las CAN se utilizan normalmente para conectar edificios en un campus universitario u otro campus grande.

[Se abre en una ventana nueva[](https://community.fs.com/es/article/complete-guide-of-campus-area-network.html)community.fs.com](https://community.fs.com/es/article/complete-guide-of-campus-area-network.html)

Red de área de campus (CAN)

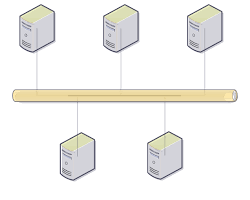
* **Red de almacenamiento (SAN)**: una red de alta velocidad que se utiliza para conectar servidores a dispositivos de almacenamiento. Las SAN se utilizan normalmente en grandes empresas donde es necesario acceder rápidamente a los datos.

[Se abre en una ventana nueva[](https://redesinformaticas.org/red-san/)redesinformaticas.org](https://redesinformaticas.org/red-san/)

Red de área de almacenamiento (SAN)

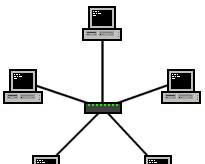
**Por topología:**

* **Bus**: una topología en la que todos los dispositivos están conectados a un único cable.

[Se abre en una ventana nueva[](https://es.wikipedia.org/wiki/Red_en_bus)es.wikipedia.org](https://es.wikipedia.org/wiki/Red_en_bus)

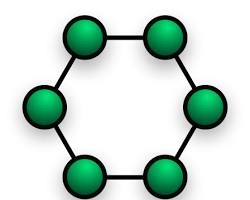
Bus topología

* **Estrella**: una topología en la que todos los dispositivos están conectados a un dispositivo central.

[Se abre en una ventana nueva[](https://es.wikipedia.org/wiki/Red_en_estrella)es.wikipedia.org](https://es.wikipedia.org/wiki/Red_en_estrella)

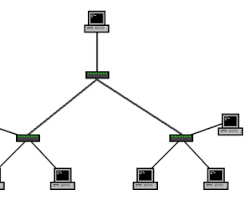
Topología de estrella

* **Anillo**: una topología en la que cada dispositivo está conectado a dos otros dispositivos, formando un anillo.

[Se abre en una ventana nueva[](https://es.wikipedia.org/wiki/Red_en_anillo)es.wikipedia.org](https://es.wikipedia.org/wiki/Red_en_anillo)

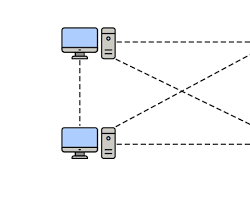
Topología de anillo

* **Árbol**: una topología en la que los dispositivos están conectados en una jerarquía, con un dispositivo en la parte superior y otros dispositivos conectados a él.

[Se abre en una ventana nueva[](https://es.wikipedia.org/wiki/Red_en_%C3%A1rbol)es.wikipedia.org](https://es.wikipedia.org/wiki/Red_en_%C3%A1rbol)

Topología de árbol

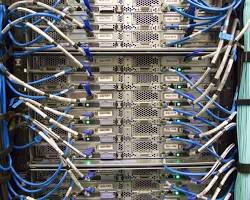
* **Malla**: una topología en la que cada dispositivo está conectado a todos los demás dispositivos.

[Se abre en una ventana nueva[](https://topologiasdered.com/red-en-malla/)topologiasdered.com](https://topologiasdered.com/red-en-malla/)

Topología de malla

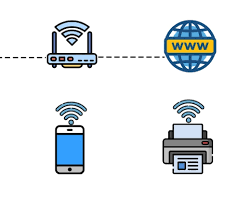
**Por medio de transmisión:**

* **Red cableada**: una red que utiliza cables para conectar dispositivos. Los cables de par trenzado, el cable coaxial y la fibra óptica son los tipos de cable más comunes que se utilizan en las redes cableadas.

[Se abre en una ventana nueva[](https://www.gadae.com/blog/crear-una-red-cableada/)www.gadae.com](https://www.gadae.com/blog/crear-una-red-cableada/)

Red cableada

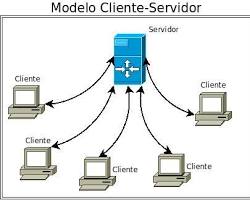
* **Red inalámbrica**: una red que utiliza ondas de radio para conectar dispositivos. Wi-Fi, Bluetooth e infrarrojos son los tipos de tecnologías inalámbricas más comunes que se utilizan en las redes inalámbricas.

[Se abre en una ventana nueva[](https://topologiasdered.com/red-inalambrica/)topologiasdered.com](https://topologiasdered.com/red-inalambrica/)

Red inalámbrica

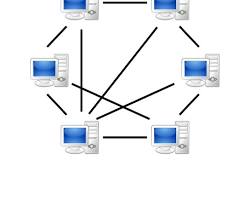
**Por relación funcional:**

* **Cliente-servidor**: una red en la que hay dispositivos cliente y dispositivos servidor. Los dispositivos cliente solicitan servicios de los dispositivos servidor.

[Se abre en una ventana nueva[](https://psp.codeandcoke.com/apuntes:sockets)psp.codeandcoke.com](https://psp.codeandcoke.com/apuntes:sockets)

Red clienteservidor

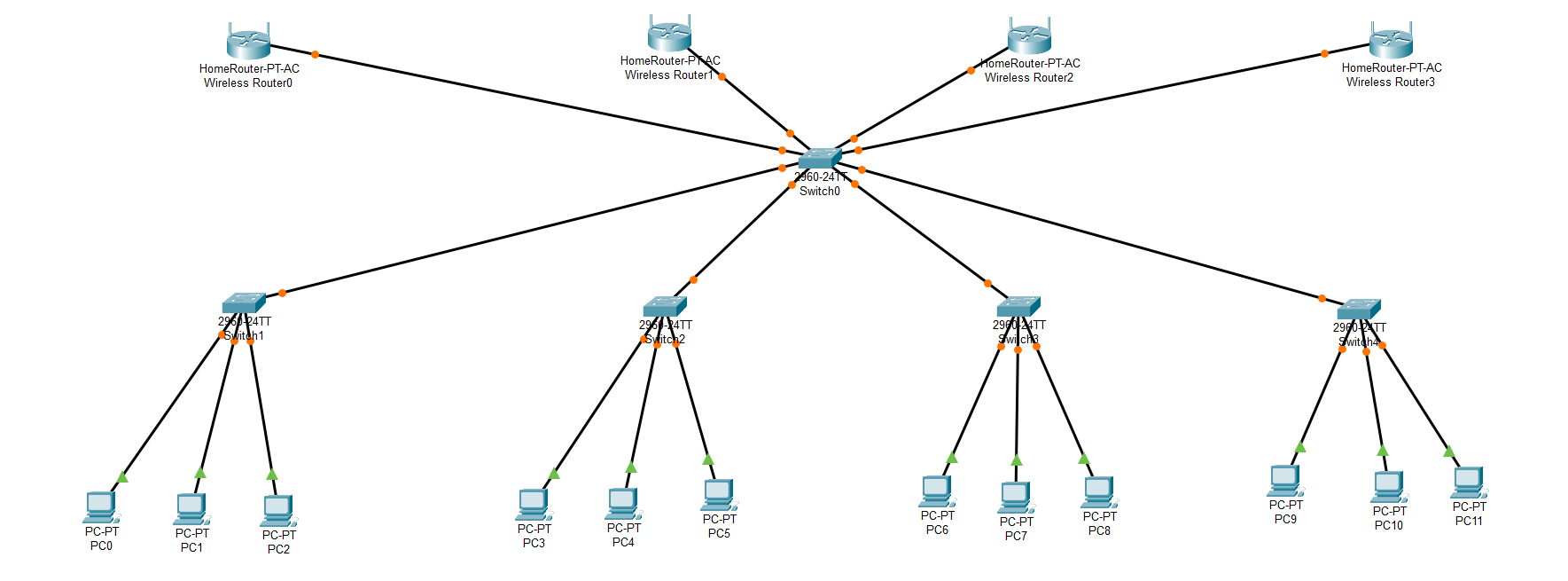
* **Igual a igual (P2P)**: una red en la que todos los dispositivos son iguales. No hay servidores ni clientes dedicados.

[Se abre en una ventana nueva[](https://es.wikipedia.org/wiki/Peer-to-peer)es.wikipedia.org](https://es.wikipedia.org/wiki/Peer-to-peer)

Red de igual a igual (P2P)

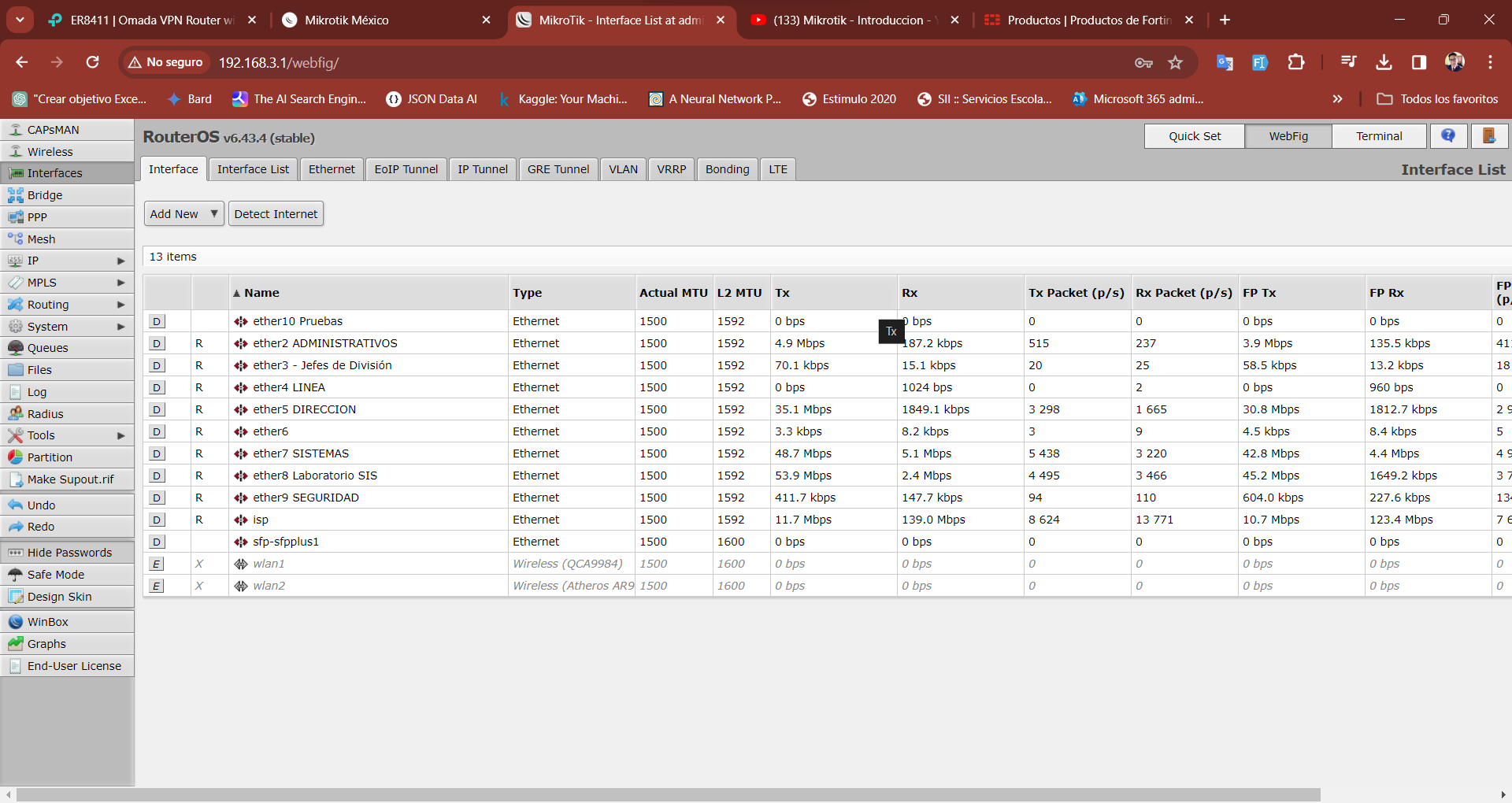
Estas son solo algunas de las formas más comunes de clasificar las redes informáticas. Hay muchas otras formas de clasificar redes, y el método específico utilizado dependerá de la situación específica".

Practica: Crear 4 Lans en un switch



Semana 4 Equipos de Networking

Router



# Semana 5 – Unidad 2 - Normas y estándares de redes de datos.

Las normas y estándares en redes de datos son fundamentales para garantizar la interoperabilidad, la seguridad y el funcionamiento eficiente de las redes de comunicación. Aquí tienes algunos de los estándares y normas más importantes en este campo:

IEEE 802: Esta es una familia de estándares desarrollados por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) que cubren una amplia gama de tecnologías de redes de área local (LAN) y redes de área amplia (WAN). Algunos subestándares notables dentro de la familia IEEE 802 incluyen:

* 802.3: Ethernet.
* 802.11: Wi-Fi.
* 802.15: Redes inalámbricas de área personal (por ejemplo, Bluetooth).
* 802.16: WiMAX.

TCP/IP (Transmission Control Protocol/Internet Protocol): Es el conjunto de protocolos que sustenta Internet y muchas redes locales. Incluye estándares como IPv4, IPv6, TCP, UDP, ICMP, FTP, HTTP, etc.

ISO/OSI (Open Systems Interconnection): Es un modelo de referencia para la comunicación de sistemas abiertos. Aunque no se implementa directamente en la práctica, sus siete capas han sido una base para el diseño de protocolos de red. No obstante, los estándares de Internet (TCP/IP) son los más comúnmente utilizados en lugar de los estándares OSI.

DNS (Domain Name System): Es un estándar que se encarga de traducir los nombres de dominio en direcciones IP y viceversa.

DHCP (Dynamic Host Configuration Protocol): Estándar que proporciona configuración dinámica de direcciones IP a dispositivos en una red.

SNMP (Simple Network Management Protocol): Estándar para la gestión de dispositivos en una red IP.

802.1X: Estándar para control de acceso a la red (NAC), que proporciona autenticación de dispositivos conectados a una red.

VLAN (Virtual LAN): Estándar que permite la segmentación lógica de una red, separando los dispositivos en diferentes dominios de broadcast.

STP/RSTP (Spanning Tree Protocol/Rapid Spanning Tree Protocol): Estándares para la prevención de bucles en redes Ethernet.

Fiber Channel: Estándar para redes de almacenamiento de datos de alta velocidad, comúnmente utilizado en entornos de almacenamiento en red (SAN).

POE (Power over Ethernet): Estándar que permite suministrar energía eléctrica a través de los cables de red Ethernet.

SSL/TLS (Secure Sockets Layer/Transport Layer Security): Estándares de seguridad para la comunicación segura a través de Internet.

El estándar IEEE 802.11, también conocido como Wi-Fi, es una familia de estándares que define las especificaciones para las redes de área local inalámbricas (WLAN). Aquí te proporciono una breve historia, así como los tipos y clasificaciones más comunes dentro del estándar:

Historia:

1997: Se lanzó la primera versión del estándar 802.11, que ofrecía tasas de transmisión de hasta 2 Mbps utilizando la modulación de espectro expandido (DSSS).

1999: Se lanzó una revisión del estándar, conocida como 802.11b, que permitía tasas de transmisión de hasta 11 Mbps utilizando la modulación por desplazamiento de fase (OFDM).

2003: Se lanzó la revisión 802.11g, que mejoraba aún más la velocidad, permitiendo tasas de transmisión de hasta 54 Mbps.

2009: Se lanzó la revisión 802.11n, que introdujo tecnologías como MIMO (Multiple Input Multiple Output) y canales de 40 MHz, permitiendo tasas de transmisión teóricas de hasta 600 Mbps.

2013: Se lanzó la revisión 802.11ac (también conocida como Wi-Fi 5), que ofrecía mejoras significativas en velocidad y rendimiento, con tasas de transmisión teóricas de hasta varios gigabits por segundo.

2019: Se lanzó la revisión 802.11ax (Wi-Fi 6), que mejora la eficiencia espectral y el rendimiento en entornos congestionados con múltiples dispositivos.

2022: Se lanzó la revisión 802.11be (Wi-Fi 7), que introduce mejoras adicionales en la velocidad, capacidad y eficiencia energética.

Tipos y Clasificaciones:

802.11a: Operaba en la banda de frecuencia de 5 GHz y ofrecía tasas de transmisión de hasta 54 Mbps.

802.11b: Operaba en la banda de frecuencia de 2.4 GHz y ofrecía tasas de transmisión de hasta 11 Mbps.

802.11g: También operaba en la banda de frecuencia de 2.4 GHz, pero ofrecía tasas de transmisión de hasta 54 Mbps.

802.11n: Operaba en ambas bandas de frecuencia (2.4 GHz y 5 GHz) y ofrecía tasas de transmisión de hasta 600 Mbps.

\*\*802

.11ac (Wi-Fi 5):\*\* Opera principalmente en la banda de frecuencia de 5 GHz y ofrece tasas de transmisión de hasta varios gigabits por segundo, dependiendo de la implementación.

802.11ax (Wi-Fi 6): También opera en ambas bandas de frecuencia y ofrece mejoras significativas en eficiencia espectral y rendimiento, especialmente en entornos densos con múltiples dispositivos.

802.11be (Wi-Fi 7): Esta es la última revisión del estándar, que ofrece mejoras adicionales en velocidad, capacidad y eficiencia energética para satisfacer las demandas de los entornos de red futuros.

Además de estas revisiones principales, también existen subtipos y variantes dentro de cada revisión que pueden diferir en características como el ancho de banda de los canales, el número de flujos espaciales (MIMO), y otras características de rendimiento y seguridad.