



S.E.P. TECNOLÓGICO NACIONAL DE MÉXICO

INSTITUTO TECNOLÓGICO De Tuxtepec

INTERCONECTIVIDAD DE REDES

TEMAS VISTOS EN CLASES

Nombre y Número de Control:

Cardoza Martínez Yasmin

22350393

DOCENTE:

JULIO AGUILAR CARMONA

CARRERA:

INGENIERÍA INFORMÁTICA

Semestre y grupo: 7A

San Juan Bautista Tuxtepec, Oaxaca.

04/ DIC/2025

PARÁMETROS DE CONFIGURACIÓN DE RED

Los parámetros clave de configuración de red son la Dirección IP, Máscara de Subred, Puerta de Enlace (Gateway) y Servidores DNS, que identifican un dispositivo, definen la red local, conectan a otras redes y traducen nombres a IPs, respectivamente. Se pueden configurar manualmente (estática) o automáticamente (DHCP), y también incluyen el Nombre de Host, Topología (física/lógica) y ajustes específicos como puertos (FTP, LPR) para aplicaciones.

Parámetros Fundamentales

- Dirección IP (IP Address): Identificador único del dispositivo en la red (ej: 192.168.1.100).
- Máscara de Subred (Subnet Mask): Determina qué parte de la IP es la red y cuál el dispositivo (ej: 255.255.255.0).
- Puerta de Enlace (Gateway): Dirección IP del router que permite la comunicación con otras redes (ej: 192.168.1.1).
- Servidores DNS: Traducen nombres de dominio (ej: www.google.com) a direcciones IP (ej: 8.8.8.8).

Métodos de Configuración

Estática: Se ingresan todos los valores manualmente.

Dinámica (DHCP): El servidor asigna la configuración automáticamente.

Configuración IP

- DHCP activado

Configura la máquina para recibir su dirección IP, su máscara de subred y su puerta de enlace predeterminada automáticamente desde un servidor DHCP.

Cuando se usa el DHCP no puede especificar manualmente la dirección IP, la máscara de subred o la puerta de enlace predeterminada.

ESTRATEGIAS DE COMPUTO PARA IDENTIFICAR SI UN EQUIPO ESTA EN LA RED O NO

En este tema vimos estrategias para identificar si un equipo está en la red, se pueden emplear varias estrategias informáticas que van desde herramientas integradas en el sistema operativo hasta aplicaciones especializadas. Estas estrategias utilizan principalmente la dirección IP y protocolos de red como ICMP y ARP para verificar la conectividad.

Estrategias y Herramientas Principales

1. Herramientas Integradas del Sistema Operativo

Son métodos rápidos que no requieren instalación de software adicional y se ejecutan desde la línea de comandos (Símbolo del sistema en Windows o Terminal en Linux/macOS).

Comando ping: Es la herramienta fundamental para probar la accesibilidad de un host. Envía paquetes de solicitud a una dirección IP o nombre de dominio específicos.

Uso: ping [dirección IP o nombre de host]

Resultado: Si recibes respuestas, el equipo está activo y accesible. Si hay "Tiempos de espera agotados para esta solicitud", puede indicar que el equipo no está en la red, está apagado o un cortafuegos está bloqueando la comunicación.

Comando arp -a: El Protocolo de resolución de direcciones (ARP) mapea direcciones IP a direcciones MAC físicas.

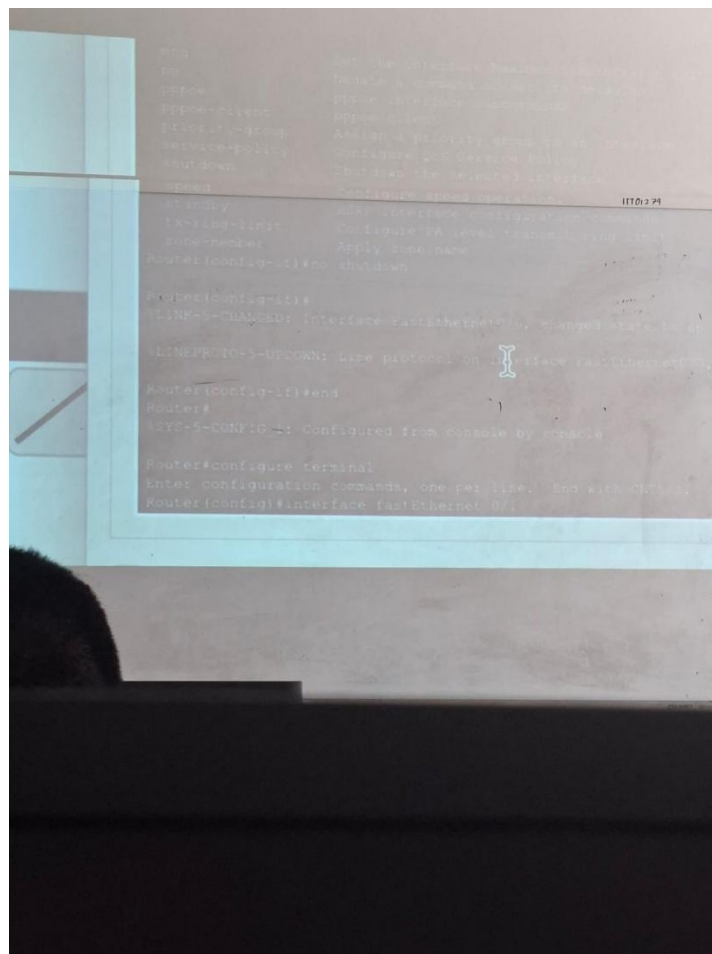
Uso: Ejecutar arp -a en la línea de comandos muestra una lista de los dispositivos actualmente conectados a tu red local (es decir, aquellos con los que tu máquina ha tenido comunicación recientemente) junto con sus direcciones MAC.

Comando ipconfig (Windows) o ifconfig / ip addr (Linux/macOS): Permite ver tu propia dirección IP y la máscara de subred, lo cual es útil para saber en qué rango de red buscar otros dispositivos.

2. Acceso a la Configuración del Router

La interfaz de administración de tu router (puerta de enlace) suele tener una sección que muestra una lista de todos los dispositivos actualmente conectados a la red local (tanto por cable como Wi-Fi).

Uso: Abre un navegador web e ingresa la dirección IP de tu router (comúnmente 192.168.1.1 o 10.0.0.1), inicia sesión con tus credenciales y busca opciones como "Dispositivos conectados", "Clientes DHCP" o "Estado de red".



CLASIFICACIONES DE DIRECCIONES IP

Como otro tema relacionado a las direcciones ip es su clasificación, en este tema se toma en cuenta que las clases de direcciones IP son categorías que clasifican las direcciones según su primer octeto y se dividen principalmente en las clases A, B, C, D y E. Las clases A, B y C se usan para redes unicast (comunicación uno a uno), mientras que la clase D se utiliza para multidifusión y la clase E se reserva para uso experimental o futuro.

Clases principales

Clase A:

- Primer octeto: entre 0 y 127.
- Máscara de subred predeterminada:
- 255.0.0.0
- Uso: Redes grandes, como las de proveedores de servicios de Internet (ISP).
- Ejemplo:
- 10.52.36.11.

Clase B:

- Primer octeto: entre 128 y 191.
- Máscara de subred predeterminada: 255.255.0.
- Uso: Redes corporativas grandes y medianas.
- Ejemplo: 172.16.52.63

Clase C:

- Primer octeto: entre 192 y 223.
- Máscara de subred predeterminada: 255.255.255.0.
- Uso: Redes más pequeñas o en redes de área local (LAN).
- Ejemplo: 192.168.123.132

Método Número Mágico

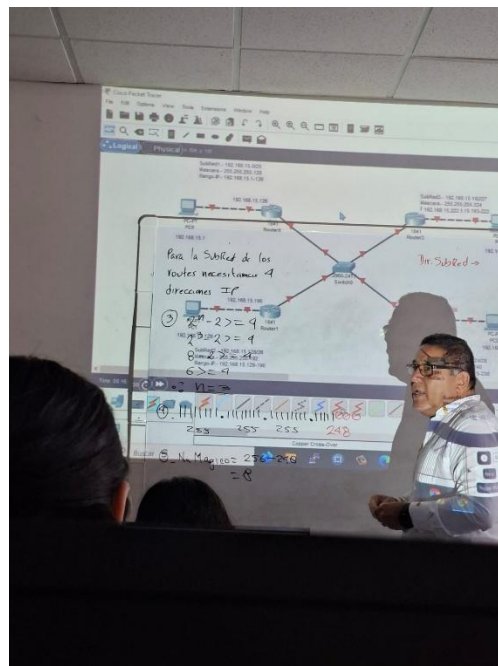
1. Identificar la Clase de IP.
2. Identificar la Máscara de Red.
3. Aplicar la Fórmula:
 $2^n \geq \text{Subredes}$
 $2^n - 2 \geq \text{Host}$
4. Obtener la Máscara de Subred.
5. Encontrar el Número Mágico.

SUBNETTING

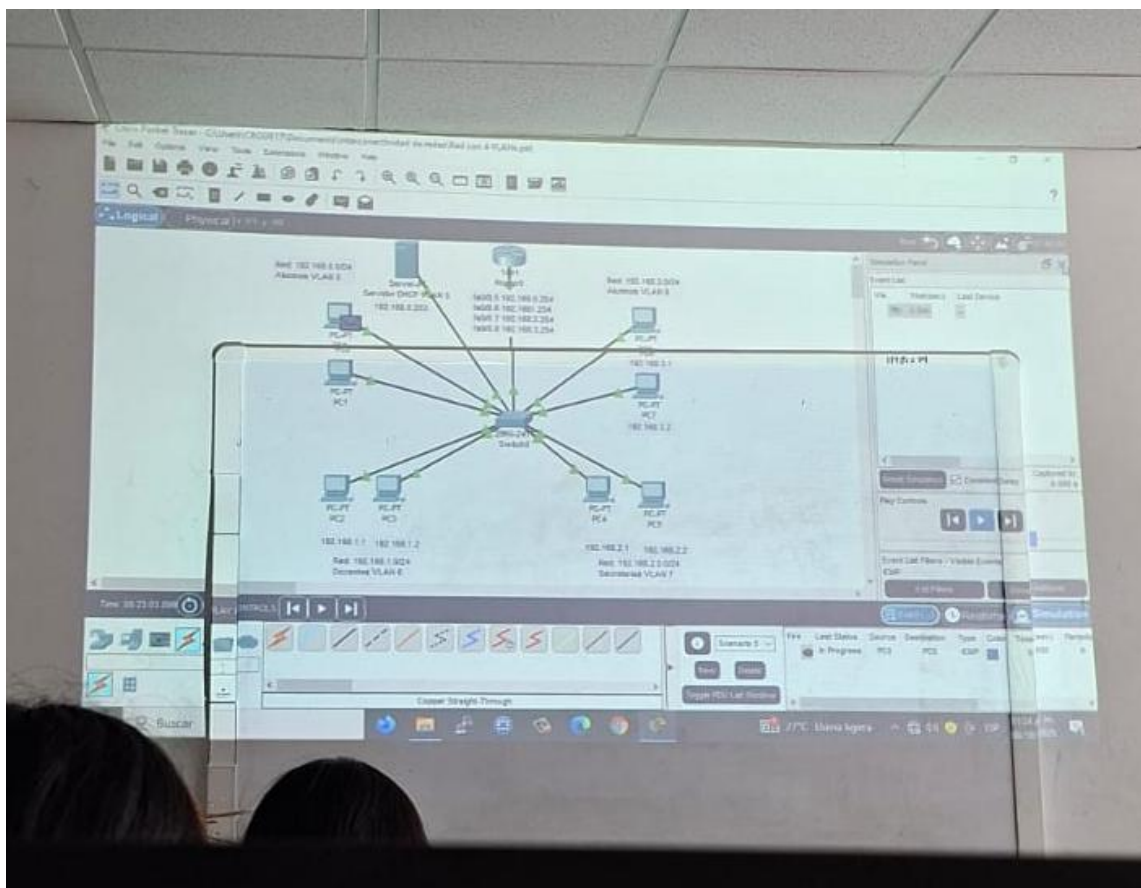
El subnetting (o subredes) es el proceso de dividir una red IP grande en múltiples redes más pequeñas y manejables. Esto se logra modificando la máscara de subred, lo que divide la red original en subredes que funcionan de forma independiente. Los beneficios principales incluyen una mejor gestión del tráfico, mayor seguridad, reducción de la congestión y una organización más eficiente de las direcciones IP.

¿Cómo funciona?

- **División de la red:** Se divide una red IP en segmentos más pequeños.
- **Máscara de subred:** Se utiliza una máscara de subred para determinar el tamaño de cada subred. Al modificar esta máscara, se "toman prestados" bits de la porción de host para crear la porción de subred.
- **Subredes independientes:** Cada subred funciona como una red individual, con sus propios dominios de broadcast, lo que limita la propagación de mensajes de difusión.
- **Enrutamiento:** Un router se encarga de conectar las subredes y enrutar el tráfico entre ellas de manera más eficiente.



SIMULACIÓN DE UNA RED LAN



ENRUTAMIENTO ESTÁTICO

El enrutamiento estático es un método de enrutamiento de red donde las rutas se configuran manualmente en un router, en lugar de ser descubiertas automáticamente por protocolos dinámicos. Esto proporciona control total y simplicidad para redes pequeñas y estables, pero requiere intervención manual del administrador y carece de la flexibilidad de los métodos dinámicos para adaptarse a cambios en la red.

Características clave

- **Configuración manual:** Un administrador define las rutas en la tabla de enrutamiento del router especificando la red de destino, la máscara de subred y la siguiente dirección de salto o la interfaz de salida.
- **Bajo overhead:** No genera tráfico de red adicional para el intercambio de información de enrutamiento, ya que no hay protocolos dinámicos comunicándose constantemente.
- **Control total:** Permite un control preciso sobre cómo se enrutan los paquetes de datos.
- **Ideal para redes pequeñas y estables:** Es fácil de implementar y gestionar en redes con topologías que cambian poco.
- **Ruta predeterminada:** Se utiliza comúnmente para crear una ruta estática predeterminada, la cual dirige el tráfico destinado a redes desconocidas a una puerta de enlace específica, como la puerta de enlace a Internet.

Ventajas

- **Control y seguridad:** Ofrece un control granular sobre el tráfico y puede mejorar la seguridad al no enviar información de enrutamiento a la red.
- **Simplicidad en redes pequeñas:** La configuración inicial es sencilla para redes con pocos routers.

- **Menor sobrecarga:** No consume ancho de banda ni recursos del router para intercambiar información de enrutamiento constantemente.
- **Convergencia predecible:** Las rutas no cambian a menos que el administrador las modifique, lo que facilita la solución de problemas.

Desventajas

- **Escalabilidad limitada:** No es práctico para redes grandes, ya que la configuración manual se vuelve tediosa y propensa a errores.
- **Poca flexibilidad:** No puede adaptarse automáticamente a fallos de enlaces o cambios en la topología de la red, lo que puede causar congestión o interrupciones.
- **Requiere intervención manual:** Cualquier cambio en la red exige una actualización manual de las tablas de enrutamiento en todos los routers afectados.

ENRUTAMIENTO DINÁMICO

El enrutamiento dinámico es un proceso automatizado que permite a los enrutadores ajustar y actualizar sus tablas de enrutamiento para dirigir el tráfico de manera eficiente en respuesta a cambios en la red, como fallas o congestión. Los enrutadores utilizan protocolos de enrutamiento dinámico para comunicarse entre sí, descubrir redes distantes y encontrar la ruta óptima para los paquetes de datos de forma autónoma, a diferencia del enrutamiento estático que requiere configuración manual. Los tipos principales de estos protocolos incluyen los de vector de distancia (como RIP), los de estado de enlace (como OSPF) y los híbridos (como EIGRP).

Características principales

- **Adaptabilidad:** Se adapta automáticamente a los cambios en la red, como la caída de un enlace, encontrando nuevas rutas sin intervención humana.
- **Eficiencia:** Optimiza las rutas basándose en factores como el tráfico y el ancho de banda, utilizando los recursos de la red de manera más eficiente.
- **Automatización:** Elimina la necesidad de intervención manual para configurar las rutas, lo que reduce los errores humanos y simplifica la administración en redes grandes.

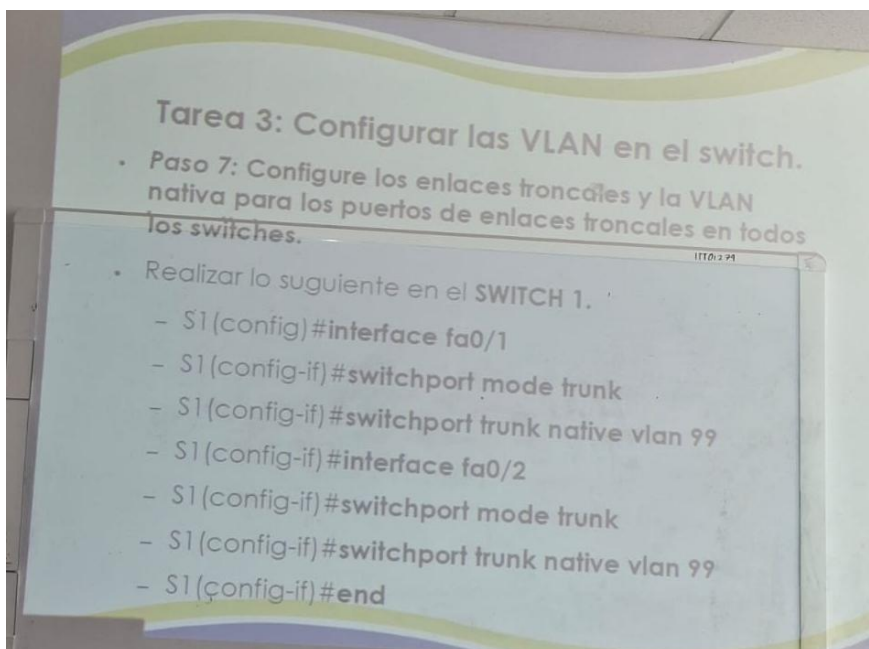
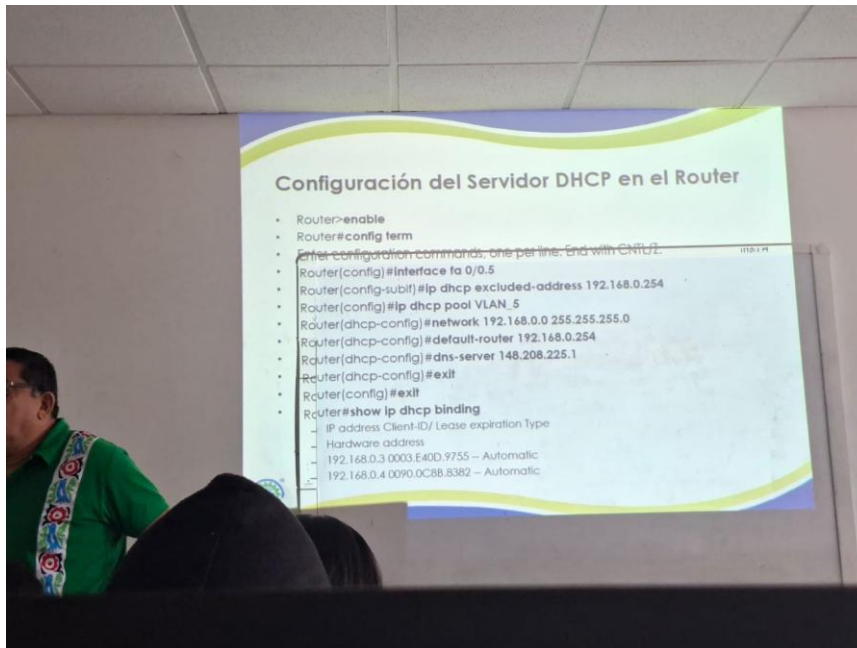
Tipos de protocolos de enrutamiento dinámico

- **Protocolos de vector de distancia:** Calculan la mejor ruta basándose en la distancia (número de saltos o métricas similares). Ejemplos: RIP.
- **Protocolos de estado de enlace:** Los enrutadores construyen un mapa completo de la red y calculan la ruta más corta basándose en este mapa. Son generalmente más rápidos y eficientes. Ejemplos: OSPF, IS-IS.
- **Protocolos híbridos:** Combinan características de los protocolos de vector de distancia y estado de enlace. Ejemplo: EIGRP.

Usos en otros campos

- **Logística:** Se utiliza para la optimización de rutas de entrega en tiempo real, teniendo en cuenta factores como el tráfico y el estado de la carretera.
- **Neurociencia:** Se refiere a la forma en que el cerebro procesa y comunica señales sensoriales y mnemónicas para tomar decisiones.

CONFIGURACIÓN DE SWITCH



La practica se hizo en cisco

REDES INALÁMBRICAS

Las redes inalámbricas son sistemas de comunicación que conectan dispositivos sin necesidad de cables, utilizando ondas de radiofrecuencia para transmitir datos entre ellos. Facilitan la movilidad y conectividad de dispositivos como ordenadores, teléfonos y tabletas, y su funcionamiento se basa en elementos como puntos de acceso (routers) y adaptadores inalámbricos en los dispositivos. Aunque ofrecen ventajas como facilidad de instalación y movilidad, presentan desafíos como la seguridad y la susceptibilidad a interferencias.

Funcionamiento y componentes

- **Uso de ondas:** Transmiten información mediante ondas de radio o infrarrojos.
- **Puntos de acceso (AP):** Actúan como puente entre la red cableada e inalámbrica, transmitiendo y recibiendo señales.
- **Adaptadores inalámbricos:** Interfaces en los dispositivos (laptops, teléfonos) que permiten la comunicación con los puntos de acceso.
- **Medio de transmisión:** El espectro radioeléctrico, que es compartido por múltiples dispositivos.

Tipos de redes inalámbricas

- **Wi-Fi:** Es el tipo más común y popular en hogares y oficinas, definido por las especificaciones 802.11 del IEEE.
- **Bluetooth:** Usado para conexiones de corto alcance entre dispositivos, como auriculares y teclados.
- **Redes Inalámbricas Metropolitanas (WMAN):** Cubren áreas más amplias, como campus universitarios o ciudades pequeñas, con un alcance de hasta 50 kilómetros.
- **IrDA (Infrarrojo):** Utiliza infrarrojos para la comunicación a muy corta distancia, como en los mandos a distancia o la transferencia de datos entre ordenadores cercanos.

Ventajas

- **Movilidad y flexibilidad:** Permiten la conexión a internet y la comunicación sin estar atado a un cable.
- **Instalación sencilla:** No requieren cableado físico, lo que facilita su configuración.
- **Accesibilidad:** Permiten que múltiples dispositivos se conecten simultáneamente sin necesidad de una conexión física.