S.E.P. TECNOLÓGICO NACIONAL DE MÉXICO

INSTITUTO TECNOLÓGICO de Tuxtepec

Int de Redes

Presenta:

Ana Dublan Zalazar

Control:

22350628

Docente:

Julio Aguilar Carmona

CARRERA:

INGENIERIA INFORMÁTICA

5/12/-2025

Introduccion

La infraestructura de Internet y de las grandes redes corporativas (WAN) depende intrínsecamente de la capacidad de sus *routers* para encontrar y mantener rutas eficientes hacia cualquier destino. En contraste con el método manual del enrutamiento estático, el enrutamiento dinámico se presenta como la solución fundamental para gestionar redes complejas y cambiantes. Esta metodología permite a los *routers* descubrir y aprender automáticamente la topología de la red, compartiendo información a través de protocolos especializados como OSPF y EIGRP. El objetivo de este trabajo es explorar los principios, las clasificaciones y la operativa de los protocolos de enrutamiento dinámico, destacando cómo su adaptabilidad y escalabilidad son esenciales para garantizar la continuidad y el rendimiento de las comunicaciones en el mundo digital moderno

Parametros 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 dispositivos, segmentan la red, conectan a otras redes e interpretan nombres de dominio, respectivamente; se configuran manualmente o automáticamente vía DHCP, y también existen ajustes de Topología (física/lógica) y de Velocidad/Dúplex para Ethernet, que determinan cómo se organizan y comunican los dispositivos.

Parámetros Fundamentales (TCP/IP)
Estos son los más comunes para la comunicación en redes basadas en IP:

Dirección IP (IPv4/IPv6): Identifica un dispositivo único en la red (ej. 192.168.1.10).

Máscara de Subred: Determina qué parte de la IP es la red y cuál es el host (ej. 255.255.255.0).

Puerta de Enlace Predeterminada (Gateway): La IP del router que permite el acceso a otras redes (Internet).

Servidores DNS: Traducen nombres de dominio a direcciones IP (ej. 8.8.8.8)

Métodos de Configuración

DHCP (Dynamic Host Configuration Protocol): El servidor asigna automáticamente los parámetros IP a los dispositivos.

Estática: Se introducen manualmente todos los parámetros en el dispositivo.

Otros Parámetros Importantes

Nombre de Host: Nombre único del equipo en la red (ej. MiPC-Oficina).

Dirección MAC: Dirección física única de la tarjeta de red.

Topología: Cómo se conectan los nodos (Estrella, Malla, Bus, etc.) y la disposición lógica.

Velocidad y Dúplex (Ethernet): Configuración de la velocidad de transmisión de datos (10/100/1000 Mbps) y si es half/full duplex.

-

¿Dónde se Configuran?

- En Configuración de Windows (Adaptadores de red).
- En la interfaz del router (para redes domésticas).
- En archivos de configuración del sistema operativo (Linux/Unix)

Estrategias de computo para identificar si un equipo esta en la red o nc

Protocolo ICMP (Internet Control Message Protocol) - El Ping

Esta es la herramienta más común y sencilla.

¿Cómo funciona?

Se envía un paquete ICMP Echo Request (solicitud de eco) al equipo objetivo usando el comando ping.

Si el equipo está encendido, conectado a la red y no está bloqueando el tráfico ICMP, responderá con un paquete ICMP Echo Reply (respuesta de eco).

Ventajas: Es rápido, universalmente soportado y fácil de usar.

Desventajas: Muchos firewalls de red o del host están configurados para bloquear el tráfico ICMP por motivos de seguridad, lo que puede dar un falso negativo (el equipo está en línea, pero no responde al ping).

Escaneo de Puertos TCP/UDP (Comúnmente con Nmap)

Esta estrategia verifica si algún servicio específico (como un servidor web, SSH o de archivos) está activo en el host.

¿Cómo funciona?

Se intenta establecer una conexión TCP (usando el "three-way handshake") o UDP a un puerto conocido (ej. puerto 80 para HTTP, 443 para HTTPS, 22 para SSH).

Si se recibe un paquete de confirmación (como un paquete SYN-ACK en TCP), el equipo está activo y ese puerto está "abierto" (o "filtrado").

Ventajas: Es más confiable que ICMP porque los servicios esenciales rara vez se bloquean por completo, y proporciona información adicional sobre qué servicios están ejecutándose.

Clasificaciones de dirección IP

Clasificación por Versión del Protocolo

- IPv4 (Internet Protocol versión 4):

Es la versión más antigua y común.

Utiliza una dirección de 32 bits, lo que permite aproximadamente 4.3 mil millones de direcciones únicas.

Se representa en formato decimal con puntos, como 192.168.1.1.

Su limitación en el número de direcciones únicas ha llevado a la necesidad de IPv6 y técnicas como NAT (Network Address Translation).

IPv6 (Internet Protocol versión 6):

Diseñado para reemplazar a IPv4 y solucionar la escasez de direcciones.

Utiliza una dirección de 128 bits, proporcionando un número virtualmente ilimitado de direcciones (aproximadamente 3.4×1038).

Se representa en formato hexadecimal con dos puntos, como 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

2. Clasificación por Ámbito de Uso

Esta es la clasificación más importante para entender la conectividad en Internet y redes locales.

Tipo de IP	**Ámbito**	**Descripción**	**Rangos Privados (IPv4)**
Pública	**Global (Internet)**	**Dirección única a nivel mundial que te identifica en Internet. Es asignada por tu ISP (Proveedor de Servicios de**	**Todas las direcciones fuera de los rangos privados.**

Tipo de IP	Ámbito	Descripción	Rangos Privados (IPv4)
		Internet) a tu *router* o dispositivo.	
Privada	Local (LAN/doméstica)	Dirección utilizada solo dentro de una red local (casa, oficina). No son únicas globalmente y no son enrutables en Internet.	Clase A: 10.0.0.0 a 10.255.255.255
		Permiten que varios dispositivos compartan una única IP pública a través de NAT.	Clase B: 172.16.0.0 a 172.31.255.255
			Clase C: 192.168.0.0 a 192.168.255.255

Subneting

El subnetting (subredes) es el proceso de dividir una red IP grande en varias redes más pequeñas y manejables, llamadas subredes.

El objetivo principal es aumentar la eficiencia y la seguridad de la red, y conservar el espacio de direcciones IP.

Conceptos Clave del Subnetting

1. Máscara de Subred (Subnet Mask)

La máscara de subred es crucial para el subnetting. Es un número de 32 bits que, al aplicarse mediante una operación lógica AND a la dirección IP, permite a un dispositivo determinar qué parte de la dirección es la parte de red y qué parte es la parte de host (dispositivo).

Bits de Red (1s): Indican la porción de la dirección que define a la subred.

Bits de Host (0s): Indican la porción de la dirección que identifica a un dispositivo específico dentro de esa subred.

2. Notación CIDR (Classless Inter-Domain Routing)

Esta es la forma más común de representar la máscara de subred. En lugar de escribir los 4 octetos, se usa una barra inclinada (/) seguida por el número total de bits que componen la porción de red.

- Ejemplo:

Una máscara de subred 255.255.255.0 tiene 24 unos (8+8+8+0).

Su representación CIDR es /24.

3. Dirección de Red

Es la primera dirección de cualquier subred. Todos los bits de host están en 0. Se utiliza para identificar la subred completa.

4. Dirección de Broadcast (Difusión)

Es la última dirección de cualquier subred. Todos los bits de host están en 1. Se utiliza para enviar un paquete a todos los dispositivos dentro de esa subred simultáneamente.

El Proceso de Subnetting

El subnetting funciona tomando bits prestados de la porción de host de la máscara de subred original y usándolos para crear nuevas subredes.

1. Determinar los Requisitos

Generalmente, el subnetting se realiza para satisfacer uno de estos dos objetivos:

Necesidad de Redes: ¿Cuántas subredes nuevas (N) necesitas?

Necesidad de Hosts: ¿Cuántos hosts (H) debe soportar cada subred?

2. Cálculo del Número de Subredes (N)

Se usa la fórmula: $2^n \geq N$, donde n es el número de bits que se van a tomar prestados de la porción de host.

Simulacion de una red LAN

Herramientas Populares para Simulación de LAN

Existen diversas herramientas, tanto de código abierto como comerciales, que te permiten diseñar, configurar y simular el tráfico en una LAN.

1. Cisco Packet Tracer

Descripción: Es el simulador más popular en entornos educativos de redes. Está diseñado por Cisco y es ideal para practicar la configuración de dispositivos Cisco (routers y switches).

Capacidades: Permite conectar virtualmente PCs, servidores, *routers*, *switches*, y dispositivos inalámbricos. Puedes aplicar protocolos como RIP, OSPF, EIGRP, DHCP y NAT.

Ventaja clave: Excelente para aprender la configuración a nivel de línea de comandos (CLI).

GNS3 (Graphical Network Simulator-3)

Descripción: Un emulador de red que permite ejecutar imágenes de sistemas operativos reales (IOS) de Cisco, Juniper y otros fabricantes en un entorno virtual. Es más avanzado y potente que Packet Tracer.

Capacidades: Simula entornos de red complejos y de gran escala. Es capaz de integrarse con software de virtualización como VMware y VirtualBox para incluir hosts con sistemas operativos completos.

Ventaja clave: Utiliza imágenes de *software* de red **reales** (no simuladas), ofreciendo resultados más cercanos a la realidad.

Enrutamiento estático

El enrutamiento estático es un método de configuración manual en un *router* para especificar una ruta a una red de destino. A diferencia del enrutamiento dinámico, donde los *routers* aprenden las rutas automáticamente a través de protocolos (como OSPF o EIGRP), en el enrutamiento estático, el administrador de la red debe ingresar cada ruta de forma individual.

¿Cómo Funciona una Ruta Estática?

Una ruta estática es básicamente una instrucción que le dice al *router* dos cosas clave:

1. **Red de Destino:** ¿A qué red quiero llegar? (Ej. 192.168.2.0/24)
2. **Siguiente Salto:** ¿Por dónde debo enviar el paquete para que llegue allí?

Existen dos maneras principales de especificar el siguiente salto:

1. Dirección del Próximo Salto (Next-Hop IP Address)

Se especifica la dirección IP del *router* vecino que está conectado a la red de destino. El *router* local realiza una búsqueda de esta dirección IP en su propia tabla ARP para encontrar la dirección MAC del vecino y enviar el paquete.

Enrutamiento dinámico

Protocolos de Enrutamiento Dinámico

Los protocolos son el "idioma" que utilizan los *routers* para intercambiar información de rutas. Se clasifican en dos grandes categorías:

1. Protocolos de Pasarela Interior (IGP - Interior Gateway Protocols)

Utilizados para intercambiar información de enrutamiento dentro de un solo Sistema Autónomo (AS), que es una red grande bajo una única administración (ej. una empresa o un campus universitario).

A. Vector Distancia (Distance Vector)

Los *routers* que usan estos protocolos comparten su tabla de enrutamiento completa con sus vecinos conectados directamente. La métrica principal suele ser el conteo de saltos (*hop count*).

Protocolo de puerta de enlace fronterizo

Sistema Autónomo (AS)

Un AS es una colección de redes IP bajo una única autoridad administrativa que ejecuta su propia política de enrutamiento interna (usando protocolos IGP como OSPF o EIGRP). Cada AS se identifica con un número único (ASN Autonomous System Number).

Función Principal

BGP se utiliza para intercambiar información de accesibilidad a la red (es decir, qué redes IP existen) entre estos diferentes AS. Su trabajo es encontrar una ruta sin bucles a través de múltiples AS hasta el destino final.

BGP vs. IGP

Mientras que los protocolos IGP (como OSPF) se centran en encontrar la ruta más rápida dentro de una sola red, BGP se centra en encontrar la ruta que cumpla con las políticas de enrutamiento y las relaciones comerciales entre las organizaciones (AS) que componen Internet.

Configuración de switch

Configuración Inicial

Antes de cualquier funcionalidad avanzada, debes configurar el acceso y la identidad del switch:

- Acceso Remoto (SSH/Telnet): Habilita el acceso seguro (idealmente SSH) a la interfaz de línea de comandos (CLI) del switch. Esto se hace asignando una dirección IP a una SVI (Interfaz Virtual de Switch), que típicamente es la VLAN 1 por defecto.
    - Comandos Típicos (Cisco):
        - interface vlan 1
        - ip address 192.168.1.10 255.255.255.0
        - no shutdown
- Nombre del Host: Asignar un nombre descriptivo (hostname) facilita la administración.

- Seguridad de Consola: Proteger el acceso físico a través del puerto de consola.

VLANs (Redes de Área Local Virtuales)

Este es el aspecto más crucial y común de la configuración de un switch moderno. Las VLANs permiten segmentar una red física en varias redes lógicas, mejorando la seguridad y el rendimiento.

- Creación de la VLAN: Se define un número y un nombre para cada grupo lógico (ej. VLAN 10 para Ventas, VLAN 20 para Ingeniería).
- Asignación de Puertos (Access Ports): Se configura un puerto específico para pertenecer a una sola VLAN. Un dispositivo conectado a este puerto solo se comunicará con otros dispositivos en la misma VLAN.
    - Comandos Típicos:
        - interface [tipo/numero_puerto]
        - switchport mode access
        - switchport access vlan 10
- Puertos Troncales (Trunk Ports):
    - Se utilizan para conectar dos switches entre sí o un switch a un *router*.
    - Permiten el paso del tráfico de múltiples VLANs a través **de un solo enlace físico.**

El protocolo de *trunking* más común es IEEE 802.1Q, que "etiqueta" (*tags*) las tramas con el ID de la VLAN.

Comandos Típicos:

interface [tipo/numero_puerto]

switchport mode trunk

switchport trunk encapsulation dot1q (si es necesario)

Seguridad de Puertos (Port Security)

Permite controlar qué dispositivos pueden conectarse a un puerto específico del switch, aumentando la seguridad de acceso.

¿Cómo funciona? Limita el número de direcciones MAC que pueden aprenderse en un puerto o especifica exactamente qué dirección MAC está permitida.

Acción de Violación: Se puede configurar la acción a tomar si se detecta una violación (ej. apagar el puerto, restringir el tráfico, o simplemente enviar una notificación).

Protocolo de Árbol de Expansión (STP - Spanning Tree Protocol)

STP es vital para prevenir bucles de Capa 2 (*switching loops*), que pueden paralizar una LAN rápidamente.

- Función: STP detecta caminos redundantes entre switches y deshabilita lógicamente los puertos que podrían causar un bucle, manteniendo solo un camino activo.

Variantes: Hay versiones más rápidas como RSTP (*Rapid Spanning Tree Protocol*) o PVST+ (*Per-VLAN Spanning Tree Plus*). Generalmente, la configuración por defecto de STP/RSTP es suficiente, pero se requiere configuración manual para influir en qué switch actúa como Root Bridge (el punto central de la red).

Redes inalámbricas

Componentes Esenciales

- Punto de Acceso (AP - Access Point): Es el dispositivo central que actúa como un puente entre la red cableada (LAN) y los clientes inalámbricos. El AP recibe los datos por cable y los transmite por aire, y viceversa.
- Adaptadores Inalámbricos: Dispositivos (integrados o externos, como tarjetas USB) instalados en los *hosts* (PCs, teléfonos) que les permiten enviar y recibir señales de radio.
- Router Inalámbrico: Un dispositivo combinado que incluye las funciones de un *router* (Capa 3), un switch (Capa 2) y un Punto de Acceso (AP). Es el dispositivo típico usado en hogares y pequeñas oficinas.

. Frecuencias de Operación

Las redes Wi-Fi operan principalmente en dos bandas de frecuencia:

- **2.4 GHz: Ofrece un mayor alcance y penetra mejor los obstáculos (paredes), pero tiene una menor velocidad**

y es más susceptible a las interferencias (por microondas, Bluetooth).

- 5 GHz: Ofrece mayor velocidad y rendimiento, pero tiene un menor alcance y es bloqueada más fácilmente por obstáculos.

Debido a que las ondas de radio viajan por el aire, la seguridad es fundamental para evitar el acceso no autorizado.

- SSID (Service Set Identifier): Es el nombre de la red inalámbrica que ves (ej. "MiCasaWi-Fi"). Ocultarlo ya no se considera una medida de seguridad efectiva.
- Autenticación y Cifrado:
    - WEP (Wired Equivalent Privacy): Protocolo obsoleto e inseguro.
    - WPA2 (Wi-Fi Protected Access 2): Actualmente el estándar mínimo. Utiliza el algoritmo AES para un cifrado fuerte.
    - WPA3: La última generación, más robusta y que ofrece un cifrado más fuerte y resistente a ataques de diccionario sin conexión

Tipos de Redes Inalámbricas

Las redes inalámbricas se clasifican según su alcance:

WPAN (Wireless Personal Area Network): Red de área personal.

Ejemplo: Bluetooth o Zigbee. Alcance de unos pocos metros.

WLAN (Wireless Local Area Network): Red de área local (Wi-Fi).

Ejemplo: Redes Wi-Fi en hogares, oficinas, o *hotspots* públicos.

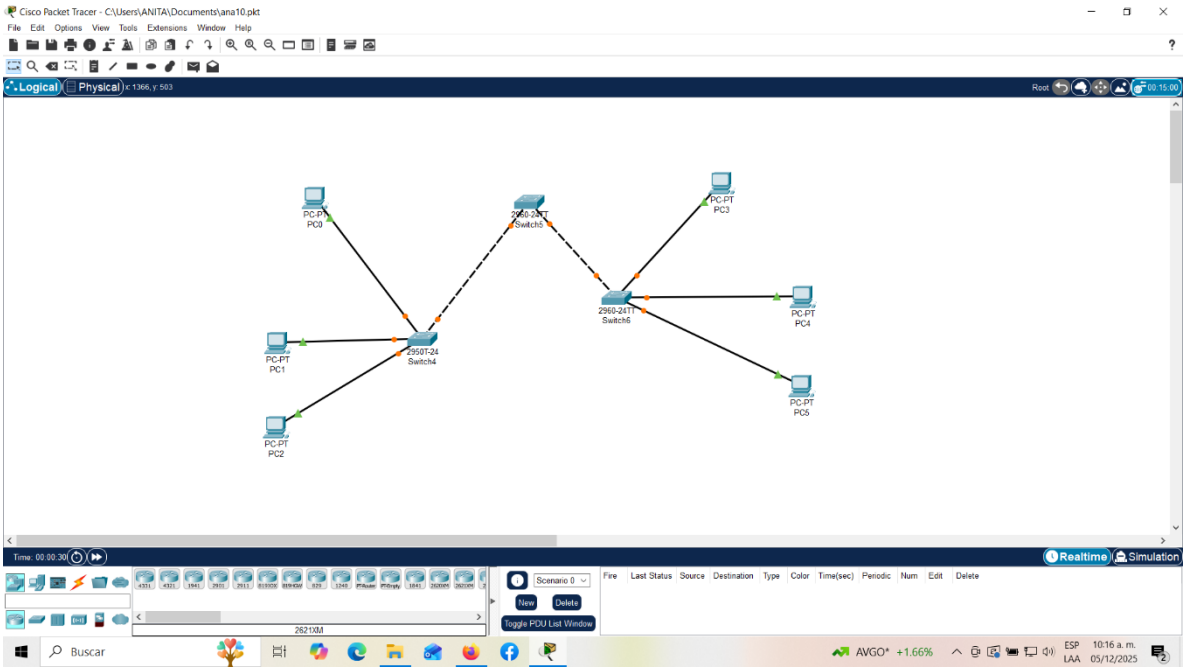
WMAN (Wireless Metropolitan Area Network): Red de área metropolitana.

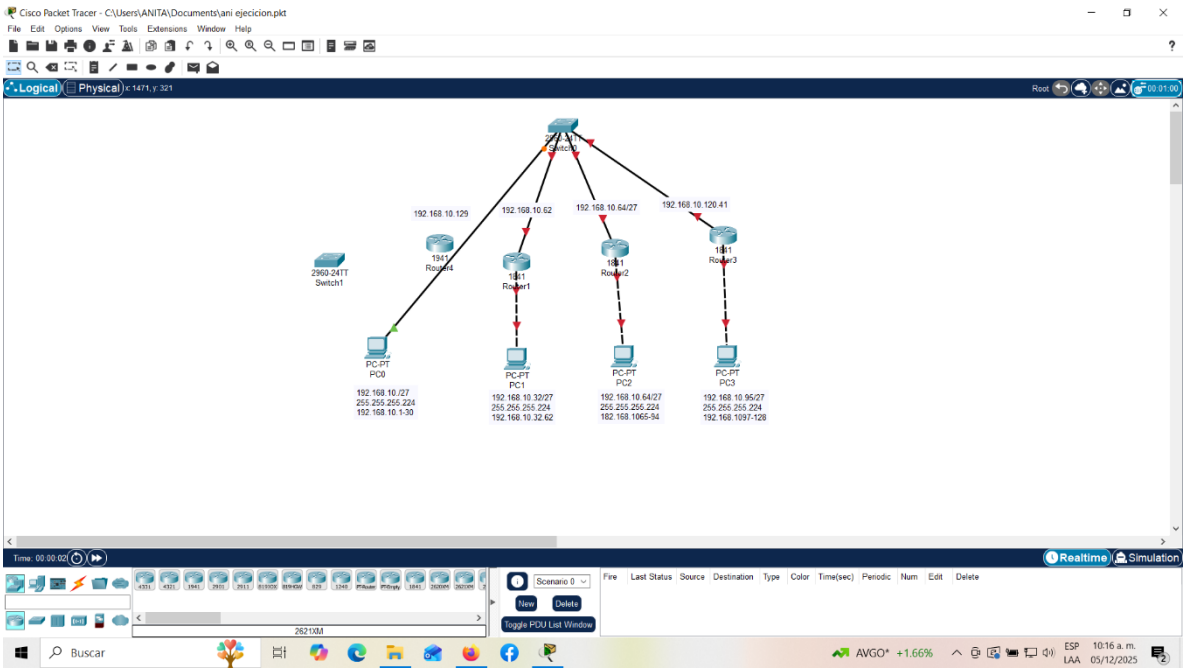
Ejemplo: WiMAX (802.16), utilizada para proporcionar acceso a Internet a una ciudad.

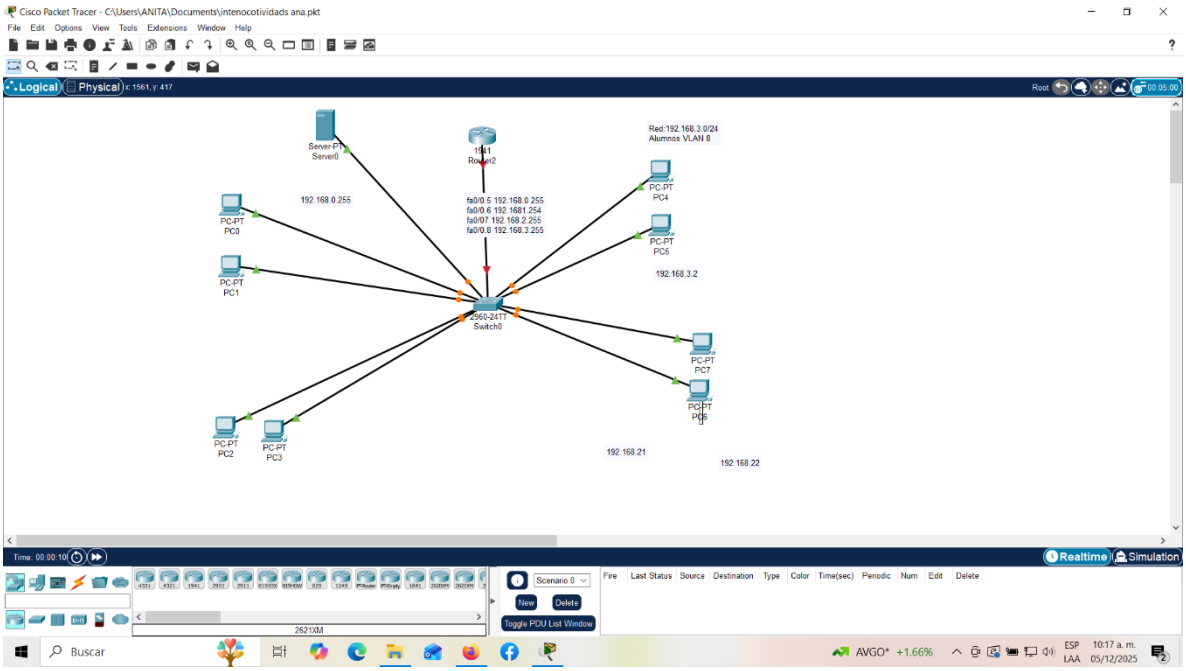
WWAN (Wireless Wide Area Network): Red de área amplia.

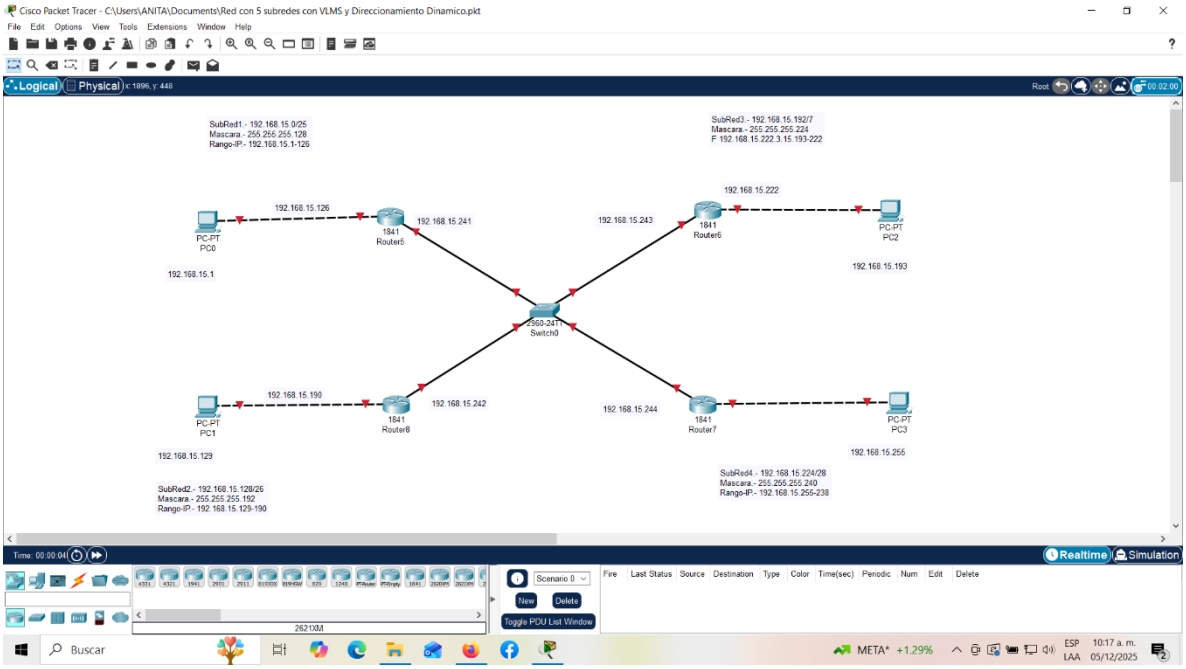
Ejemplo: Redes celulares (2G, 3G, 4G LTE, 5G), que cubren grandes regiones geográficas.

Anexo


Cisco Packet Tracer - C:\Users\ANITA\Documents\ana10.pkt
File Edit Options View Tools Extensions Window Help
Logical Physical
PC-PT PC0
2960-24TT Switch5
PC-PT PC3
2960-24TT Switch6
PC-PT PC4
PC-PT PC1
2950T-24 Switch4
PC-PT PC5
PC-PT PC2
Realtime Simulation
Buscar
AVGO* +1.66%
ESP LAA
10:16 a. m. 05/12/2025


Cisco Packet Tracer - C:\Users\ANITA\Documents\ani ejecicion.pkt
File Edit Options View Tools Extensions Window Help
Logical Physical
192.168.10.129
192.168.10.62
192.168.10.64/27
192.168.10.120.41
2960-24TT Switch1
1941 Router4
1841 Router1
1841 Router2
1841 Router3
PC-PT PC0
192.168.10./27
255.255.255.224
192.168.10.1-30
PC-PT PC1
192.168.10.32/27
255.255.255.224
192.168.10.32.62
PC-PT PC2
192.168.10.64/27
255.255.255.224
182.168.1065-94
PC-PT PC3
192.168.10.95/27
255.255.255.224
192.168.1097-128
Realtime Simulation
Buscar
AVGO* +1.66%
ESP LAA
10:16 a. m. 05/12/2025


Cisco Packet Tracer - C:\Users\ANITA\Documents\intenocotividads ana.pkt
File Edit Options View Tools Extensions Window Help
Logical Physical x: 1561, y: 417
Root
Server-PT Server0
1841 Router2
Red:192.168.3.0/24
Alumnos VLAN 8
192.168.0.255
fa0/0.5 192.168.0.255
fa0/0.6 192.168.1.254
fa0/07 192.168.2.255
fa0/0.8 192.168.3.255
PC-PT PC0
PC-PT PC1
PC-PT PC4
PC-PT PC5
192.168.3.2
2960-24TT Switch0
PC-PT PC7
PC-PT PC6
PC-PT PC2
PC-PT PC3
192.168.21
192.168.22
Time: 00:00:10
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
Delete
2621XM
Buscar
AVGO* +1.66%
ESP
LAA
10:17 a. m.
05/12/2025


Cisco Packet Tracer - C:\Users\ANITA\Documents\Red con 5 subredes con VLMS y Direccionamiento Dinamico.pkt
File Edit Options View Tools Extensions Window Help
Logical Physical x: 1896, y: 448
Root
SubRed1.- 192.168.15.0/25
Mascara.- 255.255.255.128
Rango-IP.- 192.168.15.1-126
SubRed3.- 192.168.15.192/7
Mascara.- 255.255.255.224
F 192.168.15.222.3.15.193-222
192.168.15.126
192.168.15.241
192.168.15.243
192.168.15.222
PC-PT PC0
1841 Router5
1841 Router6
PC-PT PC2
192.168.15.1
192.168.15.193
2960-24TT Switch0
192.168.15.190
192.168.15.242
192.168.15.244
PC-PT PC1
1841 Router8
1841 Router7
PC-PT PC3
192.168.15.129
192.168.15.255
SubRed2.- 192.168.15.128/26
Mascara.- 255.255.255.192
Rango-IP.- 192.168.15.129-190
SubRed4.- 192.168.15.224/28
Mascara.- 255.255.255.240
Rango-IP.- 192.168.15.255-238
Time: 00:00:04
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
Delete
2621XM
Buscar
META* +1.29%
ESP
LAA
10:17 a. m.
05/12/2025