S.E.P. TECNOLÓGICO NACIONAL DE MÉXICO

# INSTITUTO TECNOLÓGICO de Tuxtepec

ACTIVIDAD:
**REPORTE DE TODO EL SEMESTRE**

PRESENTAN:

**Oliver Santiago Isidoro**

DOCENTE:
**JULIO AGUILAR CARMONA**

CARRERA:
**INGENIERIA INFORMÁTICA**

INGENIERÍA INFORMÁTICA

**ÍNDICE**

**PARÁMETROS DE CONEXIÓN DE RED ..... 1**

**ESTRATEGIA DE EQUIPO DE CÓMPUTO EN UNA MISMA RED ..... 2**

**CLASIFICACIÓN DE DIRECCIONES IP ..... 3**

**SUBNETTING ..... 4**

**SIMULACIÓN DE UNA RED LAN ..... 5**

**ENRUTAMIENTO ESTÁTICO ..... 6**

**ENRUTAMIENTO DINÁMICO Y PROTOCOLO RIP ..... 7**

**VLANS Y CONFIGURACIÓN DE SWITCHES ..... 8**

**SIMULACIÓN DE UNA RED LAN (PRÁCTICA FINAL) ..... 9**

**DISEÑO Y SIMULACIÓN DE UNA RED INALÁMBRICA CON DHCP Y SEGURIDAD WIFI EN CISCO PACKET TRACER ..... 10**

# PARÁMETROS DE CONEXIÓN DE RED

## 1. INTRODUCCIÓN

Los parámetros de conexión de red son los ajustes esenciales que permiten que los dispositivos intercambien información dentro de una red local y se conecten a otras redes, como Internet. Una configuración adecuada asegura un funcionamiento estable, rápido, seguro y eficiente de los servicios de red.

## 2. PARÁMETROS DE CONEXIÓN DE RED

Los parámetros más importantes para la conexión de una red son:

- Dirección IP
- Máscara de subred
- Puerta de enlace
- Servidores DNS
- Velocidad y modo dúplex
- Protocolos de red

Estos elementos permiten reconocer cada dispositivo dentro de la red, determinar el tamaño o alcance de la misma y asegurar una comunicación adecuada entre los equipos conectados.

DIRECCIÓN IP

La dirección IP es un número exclusivo que se asigna a cada dispositivo para identificarlo dentro de una red. Esta dirección puede pertenecer al estándar IPv4 o IPv6, dependiendo del tipo de red que se utilice.

Ejemplo de configuración en Cisco:

```
Router(config)# interface g0/0
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# no shutdown
```

## 3. MÁSCARA DE SUBRED

**La máscara de subred se utiliza para determinar qué parte de una dirección IP identifica a la red y qué parte corresponde al dispositivo. Su función principal es permitir la segmentación de redes grandes en subredes más pequeñas y fáciles de administrar.**

**Ejemplo habitual: 255.255.255.0 (/24)**

**Ejemplo de configuración en Cisco:**

**Router(config-if)# ip address 192.168.10.1 255.255.255.0**

## 4. PUERTA DE ENLACE (GATEWAY)

**La puerta de enlace es el elemento que permite que los dispositivos de una red local puedan comunicarse con otras redes externas, como Internet. Generalmente, esta dirección corresponde a la IP del router.**

**Ejemplo:**

- **IP del equipo: 192.168.1.10**
- **Puerta de enlace: 192.168.1.1**

**Configuración de ruta por defecto en Cisco:**

**Router(config)# ip route 0.0.0.0 0.0.0.0 200.20.20.1**

## 5. SERVIDORES DNS

**El servidor DNS se encarga de traducir los nombres de dominio en direcciones IP numéricas, lo que permite una navegación más sencilla Internet sin necesidad de memorizar direcciones.**

**Configuración del DNS en Cisco:**

**Router(config)# ip name-server 8.8.8.**

**VELOCIDAD Y DÚPLEX**

**Estos parámetros determinan la rapidez con la que se transmiten los datos dentro de una red y la forma en que se realiza la comunicación entre dispositivos.**

**• Velocidad: puede ser de 10, 100 o 1000 Mbps, dependiendo del tipo de conexión y del equipo utilizado.**

**• Dúplex: define si la comunicación es en un solo sentido a la vez (half dúplex) o en ambos sentidos simultáneamente (full dúplex).**

**Ejemplo de configuración en un switch Cisco:**

**Switch(config)# interface fa0/1**

**Switch(config-if)# speed 100**

**Switch(config-if)# duplex full**

**4. PROTOCOLOS DE RED**

**Los protocolos de red son un conjunto de normas que permiten la comunicación correcta entre dispositivos dentro de una red.**

**Algunos de los protocolos más utilizados son:**

**• TCP/IP: protocolo principal que permite la comunicación en Internet.**

**• HTTP / HTTPS: utilizados para la navegación web y el acceso a páginas de Internet.**

**• DHCP: se encarga de asignar direcciones IP de forma automática a los dispositivos de la red.**

**Ejemplo de configuración de DHCP en Cisco:**

**Router(config)# ip dhcp pool RED**

**Router(dhcp-config)# network 192.168.1.0 255.255.255.0**

**Router(dhcp-config)# default-router 192.168.1.1**

**Router(dhcp-config)# dns-server 8.8.8.8**

**EJEMPLO PRÁCTICO COMPLETO CON CISCO**

**Red empresarial de tamaño reducido:**

**• Red: 192.168.50.0 /24**

**• Router: 192.168.50.1**

**Configuración del router en Cisco:**

**Router(config)# interface g0/0**

**Router(config-if)# ip address 192.168.50.1 255.255.255.0**

**Router(config-if)# no shutdown**

**Configuración del servidor DHCP:**

**Router(config)# ip dhcp pool EMPRESA**

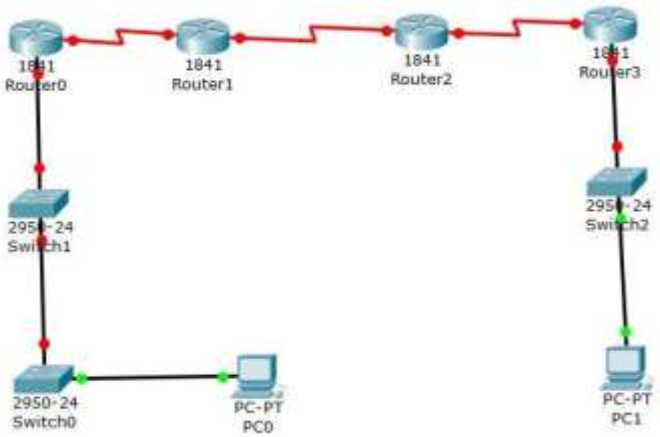
**Router(dhcp-config)# network 192.168.50.0 255.255.255.0**

**Router(dhcp-config)# default-router 192.168.50.1**

**Router(dhcp-config)# dns-server 8.8.8.8**

**Configuración de la ruta predeterminada:**

**Router(config)# ip route 0.0.0.0 0.0.0.0 200.20.20.1**



## IMPORTANCIA DE LOS PARÁMETROS DE CONEXIÓN

**Los parámetros de conexión cumplen un papel fundamental dentro de una red, ya que:**

- **Permiten la comunicación correcta entre los dispositivos**
- **Aseguran el acceso a Internet**
- **Optimizan el rendimiento de la red**
- **Evitan conflictos en el direccionamiento IP**
- **Refuerzan la seguridad de la información**

## . CONCLUSIÓN

**Los parámetros de conexión de red son indispensables para garantizar el funcionamiento adecuado de cualquier red de computadoras. Una correcta configuración, como la realizada en equipos Cisco, permite una comunicación eficiente, estable y segura. El conocimiento de estos parámetros resulta esencial para los estudiantes y profesionales del área de redes y sistemas.**

## ESTRATEGIA DE EQUIPO DE CÓMPUTO EN UNA MISMA RED

### 1. INTRODUCCIÓN

**En la actualidad, las redes de computadoras son esenciales para el funcionamiento de escuelas, empresas, hospitales y hogares. Contar con una estrategia adecuada para conectar los equipos dentro de una misma red permite que los dispositivos trabajen de manera organizada, compartan información, utilicen recursos comunes y accedan a Internet de forma eficiente.**

**Cuando los equipos se conectan sin una planeación adecuada, pueden surgir problemas como conflictos de direcciones IP, bajo rendimiento, fallas de**

**seguridad y pérdida de información. Por esta razón, es importante definir cómo se distribuirán los dispositivos, qué equipos de red se emplearán, qué tipo de direcciones IP se asignarán y qué servicios estarán disponibles.**

## . ¿QUÉ ES UNA ESTRATEGIA DE EQUIPOS EN UNA MISMA RED?

**Una estrategia de conexión en una red consiste en el diseño y planificación para interconectar distintos dispositivos, como computadoras, impresoras, servidores y puntos de acceso, dentro de una red local (LAN) de manera ordenada, segura y eficiente.**

**Esta estrategia contempla:**

- **El tipo de red que se utilizará (LAN)**
- **Los dispositivos de red necesarios (switches y routers)**
- **La correcta asignación de direcciones IP**
- **Los servicios de red disponibles (DHCP, DNS, acceso a Internet)**
- **Las medidas de seguridad para los equipos**

**El propósito principal es garantizar que todos los dispositivos se comuniquen correctamente y puedan compartir recursos sin interrupciones.**

## . ELEMENTOS PRINCIPALES DE UNA RED LOCAL

**Para que los equipos formen parte de una misma red local, se requieren los siguientes componentes:**

### 3.1 Computadoras (Hosts)

**Son los dispositivos finales que utilizan los usuarios, como computadoras de**

**escritorio y laptops.**

### 3.2 Switch

**Es el dispositivo encargado de interconectar múltiples equipos dentro de la red local.**

### 3.3 Router

**Permite la comunicación entre la red local y otras redes externas, principalmente Internet.**

### 3.4 Cables de red

**Se utilizan para realizar la conexión física entre los dispositivos, comúnmente mediante cable UTP.**

### 3.5 Software de simulación

**Cisco Packet Tracer es una herramienta que permite diseñar, configurar y probar redes en un entorno virtual sin necesidad de usar equipos físicos.**

## IMPORTANCIA DE UNA ESTRATEGIA DE RED

**Implementar una estrategia adecuada al conectar equipos dentro de una red es importante porque:**

- **Evita conflictos en la asignación de direcciones IP**
- **Mejora la velocidad y el rendimiento de la red**

**• Permite compartir archivos e impresoras**

**• Incrementa la seguridad de la información**

**• Facilita la administración y el control de la red**

## TIPO DE RED UTILIZADA

**Para conectar equipos dentro de una misma estrategia se utiliza principalmente una Red de Área Local (LAN). Este tipo de red abarca un espacio reducido, como un salón de clases, una oficina o un edificio.**

**Características de una red LAN:**

**• Alta velocidad de transmisión**

**• Bajo costo de implementación**

**• Fácil mantenimiento**

**• Capacidad para compartir recursos**

## ASIGNACIÓN DE DIRECCIONES IP

**Para que los dispositivos puedan comunicarse dentro de la red, cada uno debe contar con una dirección IP única dentro del mismo rango.**

**Ejemplo de direccionamiento:**

**• Red: 192.168.1.0**

**• Máscara: 255.255.255.0**

**Direcciones asignadas:**

**• PC1: 192.168.1.2**

**• PC2: 192.168.1.3**

**• Router: 192.168.1.1**

**ESTRATEGIA DE CONEXIÓN (TOPOLOGÍA)**

**La forma en que se conectan los dispositivos dentro de una red se conoce como topología. La más utilizada es la topología en estrella, en la cual todas las computadoras se conectan a un switch central.**

**Ventajas de la topología en estrella:**

**• Fácil administración**

**• Si un equipo falla, los demás continúan funcionando**

**• Mejor rendimiento de la red**

## 8. EJEMPLO PRÁCTICO EN CISCO PACKET TRACER (RED ESCOLAR)

### 8.1 Descripción de la red

**Se diseña una red para un salón de clases conformada por:**

**• 1 Router**

**• 1 Switch**

**• 4 Computadoras**

**La red contará con acceso a Internet y permitirá compartir recursos.**

**8.2 Dirección de la red**

**• Red: 192.168.10.0 /24**

**• Router: 192.168.10.1**

**8.3 Configuración básica del router en Cisco Packet Tracer**

**Router> enable**

**Router# configure terminal**

**Router(config)# interface g0/0**

**Router(config-if)# ip address 192.168.10.1 255.255.255.0**

**Router(config-if)# no shutdown**

**8.4 Configuración de DHCP**

**Router(config)# ip dhcp pool SALON**

**Router(dhcp-config)# network 192.168.10.0 255.255.255.0**

**Router(dhcp-config)# default-router 192.168.10.1**

**Router(dhcp-config)# dns-server 8.8.8.8**

**Con esta configuración, las computadoras reciben su dirección IP de manera automática.**

**CONEXIÓN DE LAS COMPUTADORAS AL SWITCH**

**Cada computadora se conecta físicamente al switch utilizando cable de red. En Cisco Packet Tracer se emplea el cable de cobre directo:**

**• PC → Switch**

**• Switch → Router**

**Posteriormente, cada computadora se configura en modo DHCP para obtener automáticamente su dirección IP.**

## COMPARTIR RECURSOS EN LA RED

**Una vez que los dispositivos se encuentran en la misma red, es posible compartir:**

- **Archivos**
- **Impresoras**
- **Acceso a Internet**

**Esto mejora el trabajo en equipo y reduce costos operativos.**

## SEGURIDAD DENTRO DE LA RED

**La seguridad es un aspecto fundamental dentro de la estrategia de red, e incluye:**

- **Uso de contraseñas**
- **Restricción de accesos no autorizados**
- **Control del acceso a Internet**
- **Protección de la información**

**En equipos Cisco se pueden implementar listas de control de acceso (ACL) para limitar el tráfico de red.**

## VENTAJAS DE IMPLEMENTAR UNA BUENA ESTRATEGIA DE RED

- **Mejor comunicación entre los dispositivos**
- **Mayor rapidez en las tareas**
- **Red más estable y confiable**
- **Menor cantidad de errores y fallas**
- **Mejor control de usuarios**
- **Mayor nivel de seguridad**

## . CONCLUSIÓN

**La estrategia de conexión de equipos de cómputo en una misma red es clave para el funcionamiento eficiente de cualquier organización. Una adecuada planeación permite que los dispositivos se comuniquen de forma ordenada, segura y efectiva.**

**El uso de herramientas como Cisco Packet Tracer facilita el diseño y la simulación de estas redes, permitiendo comprobar su funcionamiento antes de implementarlas en un entorno real. Comprender estos conceptos es fundamental para los estudiantes de informática y redes.**

## CLASIFICACIÓN DE DIRECCIONES IP

### 1. INTRODUCCIÓ

**Las direcciones IP son un componente esencial de las redes de computadoras, ya que permiten identificar de manera única a cada dispositivo conectado. Sin una dirección IP, un equipo no puede comunicarse con otros dispositivos ni acceder a Internet.**

**Para mejorar su organización y administración, las direcciones IP se agrupan en distintos tipos y clases. Esta clasificación facilita el diseño de redes más ordenadas, eficientes y seguras por parte de los administradores.**

## ¿QUÉ ES UNA DIRECCIÓN IP?

**Una dirección IP (Protocolo de Internet) es un identificador numérico que se asigna de forma única a cada dispositivo dentro de una red. Gracias a esta dirección, la información enviada por un equipo puede llegar correctamente a su destino.**

**Existen dos tipos principales de direcciones IP:**

- **IPv4: utiliza un formato de 32 bits representado en cuatro grupos numéricos separados por puntos (ejemplo: 192.168.1.10).**
- **IPv6: emplea un formato de 128 bits y combina números y letras (ejemplo: 2001:db8::1).**

---

## 2. CLASIFICACIÓN DE LAS DIRECCIONES IP POR CLASES

**Las direcciones IPv4 se dividen en cinco clases: A, B, C, D y E. Las más utilizadas en redes convencionales son las clases A, B y C, ya que están diseñadas para diferentes tamaños de red.**

---

### 2.1 Clase A

- **Rango: 1.0.0.0 a 126.255.255.255**
- **Máscara predeterminada: 255.0.0.0**
- **Uso: redes de gran tamaño**

**Ejemplo en Cisco Packet Tracer:**

- **IP del router: 10.0.0.1**
- **IP de la computadora: 10.0.0.2**
- **Máscara: 255.0.0.0**

---

### 2.2 Clase B

- **Rango: 128.0.0.0 a 191.255.255.255**
- **Máscara predeterminada: 255.255.0.0**
- **Uso: redes medianas**

**Ejemplo en Cisco Packet Tracer:**

- **IP del router: 172.16.0.1**
- **IP de la computadora: 172.16.0.2**

**• Máscara: 255.255.0.0**

---

**2.3 Clase C**

**• Rango: 192.0.0.0 a 223.255.255.255**

**• Máscara predeterminada: 255.255.255.0**

**• Uso: redes pequeñas**

**Ejemplo en Cisco Packet Tracer:**

**• IP del router: 192.168.1.1**

**• IP de la computadora: 192.168.1.10**

**• Máscara: 255.255.255.0**

---

**2.4 Clase D**

**• Rango: 224.0.0.0 a 239.255.255.255**

**• Uso: transmisión multicast (envío de datos a varios dispositivos simultáneamente)**

**Este tipo de direcciones no se asigna a computadoras comunes.**

---

**2.5 Clase E**

**• Rango: 240.0.0.0 a 255.255.255.255**

**• Uso: investigación y uso experimental**

**No se utilizan en redes comerciales.**

---

**3. DIRECCIONES IP PÚBLICAS Y PRIVADAS**

**3.1 Direcciones IP Públicas**

**Son las direcciones empleadas para identificar dispositivos directamente en Internet. Estas direcciones son asignadas por los proveedores de servicios de Internet (ISP) y son únicas a nivel mundial.**

---

**3.2 Direcciones IP Privadas**

**Se utilizan dentro de redes locales y no se enrutan de forma directa en Internet.**

**Rangos de direcciones privadas:**

**• 10.0.0.0 a 10.255.255.255**

**• 172.16.0.0 a 172.31.255.255**

**• 192.168.0.0 a 192.168.255.255**

**Ejemplo en Cisco Packet Tracer:**

**• Red local: 192.168.0.0**

**• Router: 192.168.0.1**

**• Computadora: 192.168.0.2**

---

**4. DIRECCIÓN IP ESTÁTICA Y DINÁMICA**

**4.1 Dirección IP Estática**

**Es una dirección que se asigna manualmente a un dispositivo y permanece fija, sin cambios.**

**Ejemplo: una impresora de red configurada con una IP permanente.**

---

**4.2 Dirección IP Dinámica**

**Es una dirección que se asigna de forma automática a través de un servidor DHCP.**

**Ejemplo de configuración DHCP en Cisco:**

**Router(config)# ip dhcp pool RED**

**Router(dhcp-config)# network 192.168.1.0 255.255.255.0**

**Router(dhcp-config)# default-router 192.168.1.1**

---

**5. DIRECCIÓN IP DE RED Y DIRECCIÓN DE BROADCAST**

**• Dirección de red: identifica a toda la red (ejemplo: 192.168.1.0).**

**• Dirección de broadcast: se utiliza para enviar información a todos los dispositivos de la red (ejemplo: 192.168.1.255).**

**Estas direcciones están reservadas y no se asignan a equipos finales.**

---

**6. EJEMPLO COMPLETO EN CISCO PACKET TRACER**

**Se diseña una red sencilla compuesta por:**

**• 1 Router**

**• 1 Switch**

**• 2 Computadoras**

**Configuración del router:**

**Router(config)# interface g0/0**

**Router(config-if)# ip address 192.168.5.1 255.255.255.0**

**Router(config-if)# no shutdown**

**Configuración de las computadoras:**

**• PC1: 192.168.5.2**

**• PC2: 192.168.5.3**

**• Gateway: 192.168.5.1**

**Con esta configuración, ambas computadoras pueden comunicarse sin problemas dentro de la red.**

**7. IMPORTANCIA DE LA CLASIFICACIÓN DE LAS DIRECCIONES IP**

**La clasificación de las direcciones IP es importante porque:**

**• Permite una mejor organización de las redes**

**• Facilita la conexión a Internet**

**• Evita conflictos entre dispositivos**

**• Simplifica la administración de la red**

**• Contribuye a mejorar la seguridad**

**8. CONCLUSIÓN**

**La clasificación de las direcciones IP es un tema clave dentro de las redes de computadoras, ya que permite comprender cómo se asignan y utilizan las direcciones para la comunicación entre dispositivos.**

**Gracias al uso de herramientas como Cisco Packet Tracer, estos conceptos pueden aplicarse de forma práctica mediante simulaciones. Comprender la clasificación de las direcciones IP es fundamental para los estudiantes de informática, redes y sistemas computacionales.**

**SUBNETTING**

**1. INTRODUCCIÓN**

**El subnetting es un proceso esencial en el diseño de redes de computadoras, ya que permite dividir una red grande en varias subredes más pequeñas. Esto mejora el rendimiento, facilita la administración y fortalece la seguridad de la red.**

**En entornos reales como escuelas, oficinas y empresas, el subnetting se utiliza para separar departamentos, controlar el tráfico de red y optimizar el uso de las direcciones IP. En este apartado se explica el concepto de subnetting y se presentan ejemplos prácticos utilizando Cisco Packet Tracer.**

## 2. ¿QUÉ ES SUBNETTING?

**Subnetting es la técnica que consiste en dividir una red IP en diferentes subredes, utilizando bits de la parte de host como parte de red. Cada subred funciona como una red independiente.**

**Ejemplo:**

- **Red original: 192.168.1.0 /24**
- **Subredes: 192.168.1.0 /26, 192.168.1.64 /26, entre otras**

**Esto permite que distintos grupos de usuarios trabajen en redes separadas dentro de la misma infraestructura.**

## 3. ¿PARA QUÉ SIRVE EL SUBNETTING?

**El subnetting se utiliza para:**

- **Aprovechar mejor las direcciones IP**
- **Reducir el tráfico de red**
- **Incrementar la seguridad**
- **Separar áreas o departamentos**
- **Mejorar el rendimiento**
- **Facilitar la administración**

## 4. CONCEPTOS BÁSICOS DEL SUBNETTING

### 4.1 Dirección de red

**Identifica a la subred completa.**

### 4.2 Dirección de broadcast

**Permite enviar información a todos los dispositivos de una subred.**

### 4.3 Máscara de subred

**Indica qué parte de la dirección IP corresponde a la red y cuál al host.**

### 4.4 Prefijo CIDR

**Forma abreviada de representar la máscara de subred, por ejemplo:**

**• /24 = 255.255.255.0**

**• /26 = 255.255.255.192**

**5. EJEMPLO DE SUBNETTING PASO A PASO**

**Red original:**

**• 192.168.10.0 /24**

**Objetivo: crear 4 subredes.**

**Paso 1: Bits necesarios**

**Para crear 4 subredes se requieren 2 bits ($2^2 = 4$).**

**Paso 2: Nueva máscara**

**/24 + 2 = /26**

**Nueva máscara: 255.255.255.192**

**Paso 3: Tamaño de subred**

**256 – 192 = 64 direcciones por subred.**

**Paso 4: Subredes resultantes**

**192.168.10.0 /26**

**Hosts: 192.168.10.1 – 192.168.10.62**

**Broadcast: 192.168.10.63**

**192.168.10.64 /26**

**Hosts: 192.168.10.65 – 192.168.10.126**

**Broadcast: 192.168.10.127**

**192.168.10.128 /26**

**Hosts: 192.168.10.129 – 192.168.10.190**

**Broadcast: 192.168.10.191**

**192.168.10.192 /26**

**Hosts: 192.168.10.193 – 192.168.10.254**

**Broadcast: 192.168.10.255**

**6. VENTAJAS DEL SUBNETTING**

**• Mejor organización de la red**

**• Mayor nivel de seguridad**

**• Menor congestión del tráfico**

**• Uso eficiente de direcciones IP**

**• Facilita la detección de fallas**

**• Mejor control del acceso**

**7. DESVENTAJAS DEL SUBNETTING**

**• Requiere conocimientos técnicos**

**• Una mala configuración puede generar fallas**

**• Implica mayor tiempo de planeación**

**8. CONCLUSIÓN**

**El subnetting es una herramienta fundamental en el diseño de redes modernas, ya que permite dividir una red amplia en subredes más pequeñas, eficientes y seguras.**

**SIMULACIÓN DE UNA RED LAN**

**1. INTRODUCCIÓN**

**Las redes de área local (LAN) permiten la comunicación entre computadoras y otros dispositivos dentro de un espacio físico reducido, como un salón, una oficina o un edificio. La simulación de una red LAN es una práctica esencial para comprender el funcionamiento de las conexiones, el direccionamiento IP y los servicios de red.**

**2. ¿QUÉ ES UNA RED LAN?**

**Una red LAN es un sistema que conecta varios dispositivos dentro de una zona limitada, como una casa, una escuela o una empresa.**

**Características principales:**

**• Alta velocidad de transmisión**

**• Bajo costo de implementación**

**• Uso de conexiones cableadas o inalámbricas**

**• Compartición de recursos como archivos, impresoras y acceso a Internet**

**3. ¿QUÉ ES LA SIMULACIÓN DE UNA RED?**

**La simulación de redes consiste en crear un modelo virtual de una red real mediante un software especializado. Esto permite:**

**• Probar configuraciones**

**• Detectar errores**

**• Aprender sin riesgos**

**• Evitar daños en equipos físicos**

**Cisco Packet Tracer es una herramienta que permite simular redes de forma gráfica e interactiva.**

**4. ELEMENTOS UTILIZADOS EN LA SIMULACIÓN**

**Para simular una red LAN se utilizan los siguientes componentes:**

**• Computadoras**

**• Switch**

**• Router**

**• Cables de red**

**• Software de simulación (Cisco Packet Tracer)**

**Cada elemento cumple una función específica dentro de la red.**

**5. TOPOLOGÍA DE LA RED LAN**

**La topología utilizada es la topología en estrella, donde todos los dispositivos se conectan a un switch central.**

**Ventajas:**

**• Fácil mantenimiento**

**• Mayor estabilidad**

**• Si un dispositivo falla, la red continúa operando**

**• Mejor control del tráfico**

**6. DISEÑO DE LA RED A SIMULAR**

**La red diseñada para la simulación incluye:**

**• 1 Router**

**• 1 Switch**

**• 3 Computadoras**

**Direcciones de red:**

**• Red: 192.168.1.0**

**• Máscara: 255.255.255.0**

**• Router: 192.168.1.1**

**• PC1: 192.168.1.2**

**• PC2: 192.168.1.3**

**• PC3: 192.168.1.4**

**7. CONFIGURACIÓN DEL ROUTER EN LA SIMULACIÓN**

**La configuración del router en Cisco Packet Tracer se realiza mediante comandos:**

**Router> enable**

**Router# configure terminal**

**Router(config)# interface g0/0**

**Router(config-if)# ip address 192.168.1.1 255.255.255.0**

**Router(config-if)# no shutdown**

**Esto permite que el router funcione como puerta de enlace de la red.**

**8. CONFIGURACIÓN DE LAS COMPUTADORAS**

**Cada computadora se configura con los siguientes parámetros:**

**PC1:**

**• IP: 192.168.1.2**

**• Máscara: 255.255.255.0**

**• Puerta de enlace: 192.168.1.1**

**PC2:**

**• IP: 192.168.1.3**

**• Máscara: 255.255.255.0**

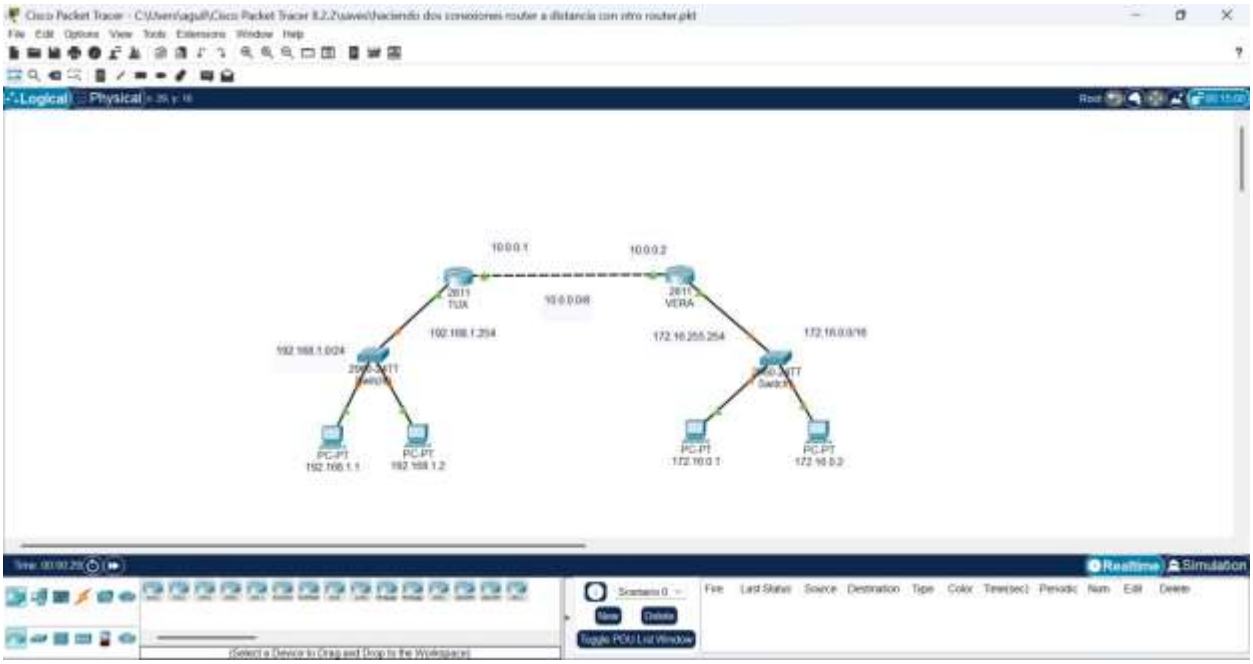
**• Puerta de enlace: 192.168.1.1**

**PC3:**

**• IP: 192.168.1.4**

**• Máscara: 255.255.255.0**

**• Puerta de enlace: 192.168.1.1**




**VENTAJAS DE LA SIMULACIÓN DE UNA RED LAN**

- **Permite aprender sin necesidad de utilizar equipos físicos reales**
- **Evita daños en los dispositivos de laboratorio**
- **Facilita la realización de prácticas y ejercicios**
- **Ayuda a identificar y corregir errores de configuración**
- **Disminuye los costos de implementación y pruebas**

## 2. APLICACIÓN DE LA SIMULACIÓN EN LA VIDA REAL

**La simulación de redes LAN se emplea en distintos ámbitos, por ejemplo:**

- **Capacitación de estudiantes y personal técnico**
- **Planeación y diseño de redes empresariales**
- **Pruebas previas a la instalación de una red real**
- **Análisis y solución de problemas de conectividad**

## 3. CONCLUSIÓN

**La simulación de una red LAN es una herramienta clave para el estudio de las redes de computadoras. Mediante programas como Cisco Packet Tracer es posible diseñar, configurar y comprobar el funcionamiento de una red de forma segura y eficiente desde una PC.**

**Estas prácticas permiten entender mejor cómo operan los dispositivos de red, cómo se usan las direcciones IP y cómo se comunican los equipos entre sí, fortaleciendo los conocimientos en informática y telecomunicaciones.**

## ENRUTAMIENTO ESTÁTICO

### 1. INTRODUCCIÓN

**El enrutamiento es el procedimiento mediante el cual los datos se trasladan de una red a otra a través de dispositivos llamados routers. Uno de los tipos más importantes es el enrutamiento estático, el cual se establece manualmente por el administrador de la red.**

**Este tipo de enrutamiento se utiliza sobre todo en redes pequeñas o medianas donde la estructura de las rutas se mantiene casi sin cambios.**

### 2. ¿QUÉ ES EL ENRUTAMIENTO ESTÁTICO?

**El enrutamiento estático consiste en definir de manera manual las rutas que se guardan en un router. En otras palabras, el administrador especifica exactamente por qué camino debe viajar el tráfico para llegar a una red determinada.**

**A diferencia del enrutamiento dinámico, el enrutamiento estático no emplea protocolos que actualicen las rutas automáticamente, por lo que cualquier modificación debe realizarse a mano.**

### 3. CARACTERÍSTICAS DEL ENRUTAMIENTO ESTÁTICO

- **Las rutas se crean y modifican manualmente**
- **No genera tráfico adicional de actualización en la red**
- **Suele ser más seguro que el enrutamiento dinámico**

**• Es sencillo de aplicar en redes de tamaño reducido**

**• No se ajusta en forma automática ante cambios en la topología**

## 4. VENTAJAS Y DESVENTAJAS

**Ventajas:**

**• Ofrece mayor control sobre el flujo de tráfico**

**• Proporciona un nivel de seguridad más alto**

**• No consume ancho de banda extra para el intercambio de rutas**

**• Es fácil de configurar en redes pequeñas**

**Desventajas:**

**• Se vuelve complicado de administrar en redes grandes**

**• No se actualiza solo cuando ocurre un cambio**

**• Requiere más tiempo de configuración y mantenimiento**

**• Si una ruta deja de funcionar, no existe una alternativa automática**

## 5. ESCENARIO DE LA SIMULACIÓN (AJUSTADO A LA IMAGEN)

**La topología simulada está formada por cuatro redes LAN con máscara /27 conectadas a un switch central, el cual enlaza a cuatro routers. Cada router proporciona servicio a una PC distinta.**

**Se aplica subnetting sobre la red 192.168.10.0/24, dividiéndola en varias subredes /27, tal como se aprecia en la imagen:**

**• Subred 1: 192.168.10.0 /27**

**• Subred 2: 192.168.10.32 /27**

**• Subred 3: 192.168.10.64 /27**

**• Subred 4: 192.168.10.96 /27**

**• Red troncal entre routers y switch: 192.168.10.128 /27**

## 6. DIRECCIONAMIENTO IP SEGÚN LA IMAGEN

### PC0

**• IP: 192.168.10.1**

**• Máscara: 255.255.255.224**

**• Gateway: 192.168.10.30**

**• Subred: 192.168.10.0 /27**

### PC1

**• IP: 192.168.10.33**

**• Máscara: 255.255.255.224**

**• Gateway: 192.168.10.62**

**• Subred: 192.168.10.32 /27**

### PC2

**• IP: 192.168.10.65**

**• Máscara: 255.255.255.224**

**• Gateway: 192.168.10.94**

**• Subred: 192.168.10.64 /27**

### PC3

**• IP: 192.168.10.97**

**• Máscara: 255.255.255.224**

• **Gateway: 192.168.10.126**

• **Subred: 192.168.10.96 /27**

**Router0**

• **G0/0 (LAN): 192.168.10.30 /27**

• **G0/1 (hacia el switch): 192.168.10.129 /27**

**Router1**

• **G0/0 (LAN): 192.168.10.62 /27**

• **G0/1 (hacia el switch): 192.168.10.130 /27**

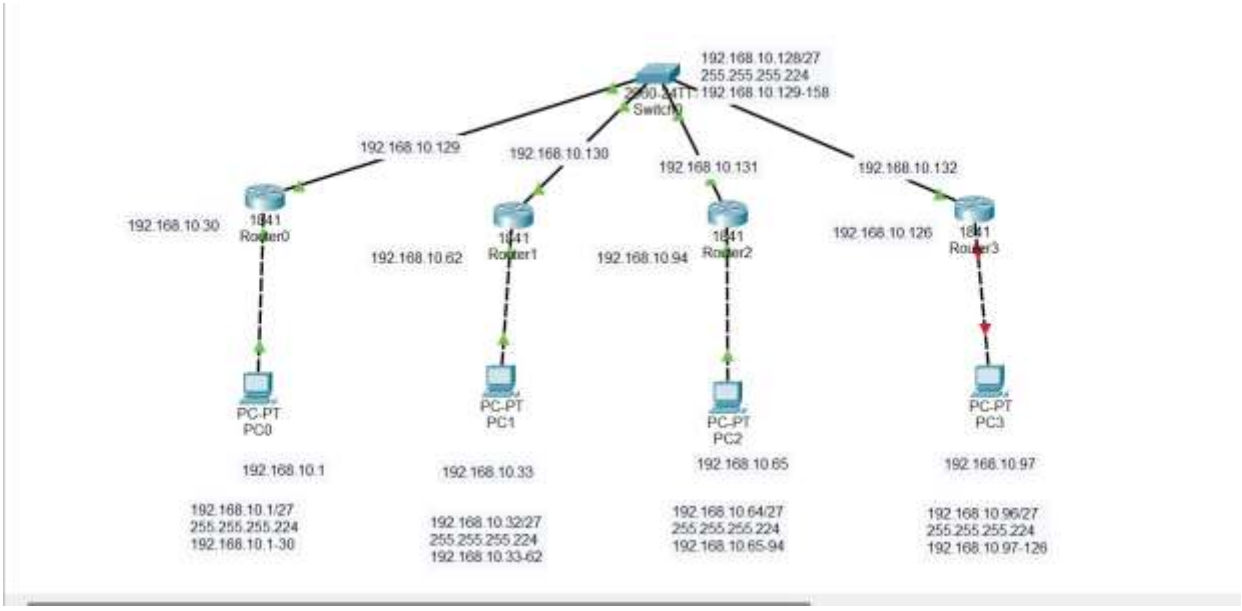
**Router2**

• **G0/0 (LAN): 192.168.10.94 /27**

• **G0/1 (hacia el switch): 192.168.10.131 /27**

**Router3**

• **G0/0 (LAN): 192.168.10.126 /27**




• **G0/1 (hacia el switch): 192.168.10.132 /27**

## 1. CONFIGURACIÓN DE LOS ROUTERS (AJUSTADA A LA IMAGEN)

**Router0**

```
enable
configure terminal
interface g0/0
ip address 192.168.10.30 255.255.255.224
no shutdown
interface g0/1
ip address 192.168.10.129 255.255.255.224
no shutdown
```

**Router1**

```
enable
configure terminal
interface g0/0
ip address 192.168.10.62 255.255.255.224
no shutdown
interface g0/1
ip address 192.168.10.130 255.255.255.224
no shutdown
```

**Router2**

```
enable
configure terminal
interface g0/0
ip address 192.168.10.94 255.255.255.224
no shutdown
interface g0/1
ip address 192.168.10.131 255.255.255.224
```

no shutdown

**Router3**

enable

configure terminal

interface g0/0

ip address 192.168.10.126 255.255.255.224

no shutdown

interface g0/1

ip address 192.168.10.132 255.255.255.224

no shutdown

---

## 2. CONFIGURACIÓN DE RUTAS ESTÁTICAS (SEGÚN LA IMAGEN)

En todos los routers se deben crear rutas estáticas hacia las otras subredes usando como **siguiente salto la red troncal 192.168.10.128/27**.

**En Router0**

ip route 192.168.10.32 255.255.255.224 192.168.10.130

ip route 192.168.10.64 255.255.255.224 192.168.10.131

ip route 192.168.10.96 255.255.255.224 192.168.10.132

**En Router1**

ip route 192.168.10.0 255.255.255.224 192.168.10.129

ip route 192.168.10.64 255.255.255.224 192.168.10.131

ip route 192.168.10.96 255.255.255.224 192.168.10.132

**En Router2**

ip route 192.168.10.0 255.255.255.224 192.168.10.129

ip route 192.168.10.32 255.255.255.224 192.168.10.130

ip route 192.168.10.96 255.255.255.224 192.168.10.132

**En Router3**

ip route 192.168.10.0 255.255.255.224 192.168.10.129

ip route 192.168.10.32 255.255.255.224 192.168.10.130

ip route 192.168.10.64 255.255.255.224 192.168.10.131

**3. VERIFICACIÓN DE CONECTIVIDAD**

Se debe hacer ping entre todas las PCs, por ejemplo desde PC0:

ping 192.168.10.33

ping 192.168.10.65

ping 192.168.10.97

Si las rutas están correctas, todas las pruebas serán exitosas.

## 4. CONCLUSIÓN

El enrutamiento estático aplicado en esta topología permite la comunicación entre cuatro subredes diferentes usando una red troncal común. La simulación representa un escenario realista de segmentación de red mediante subnetting /27.

Cisco Packet Tracer facilita la visualización del funcionamiento de las rutas estáticas, permitiendo validar direcciones IP, puertas de enlace y comunicación entre equipos antes de su implementación en un entorno real.

El enrutamiento estático es una técnica fundamental en redes de computadoras, especialmente en escenarios donde la topología es simple y se requiere un alto control del tráfico.

# ENRUTAMIENTO DINÁMICO Y PROTOCOLO RIP

## 1. INTRODUCCIÓN

El enrutamiento dinámico es un proceso automático que permite a los routers intercambiar información entre ellos para conocer las mejores rutas hacia las diferentes redes. A diferencia del enrutamiento estático, este tipo de enrutamiento se adapta automáticamente a los cambios en la topología.

Uno de los protocolos más sencillos de enrutamiento dinámico es RIP (Routing Information Protocol). En este reporte se explica el funcionamiento del enrutamiento dinámico y del protocolo RIP, utilizando una simulación en Cisco Packet Tracer para PC, basada en la topología proporcionada.

## 2. ¿QUÉ ES EL ENRUTAMIENTO DINÁMICO?

El enrutamiento dinámico es el método mediante el cual los routers aprenden automáticamente las rutas disponibles en la red mediante el uso de protocolos de enrutamiento. Estos protocolos permiten que los routers compartan información sobre las redes que conocen.

Este tipo de enrutamiento se utiliza principalmente en redes medianas y grandes, ya que reduce el trabajo del administrador y mejora la tolerancia a fallas.

## 3. CARACTERÍSTICAS DEL ENRUTAMIENTO DINÁMICO

- Aprendizaje automático de rutas
- Actualización constante de la tabla de enrutamiento
- Capacidad de adaptarse a fallas
- Menor intervención manual
- Uso de protocolos de enrutamiento

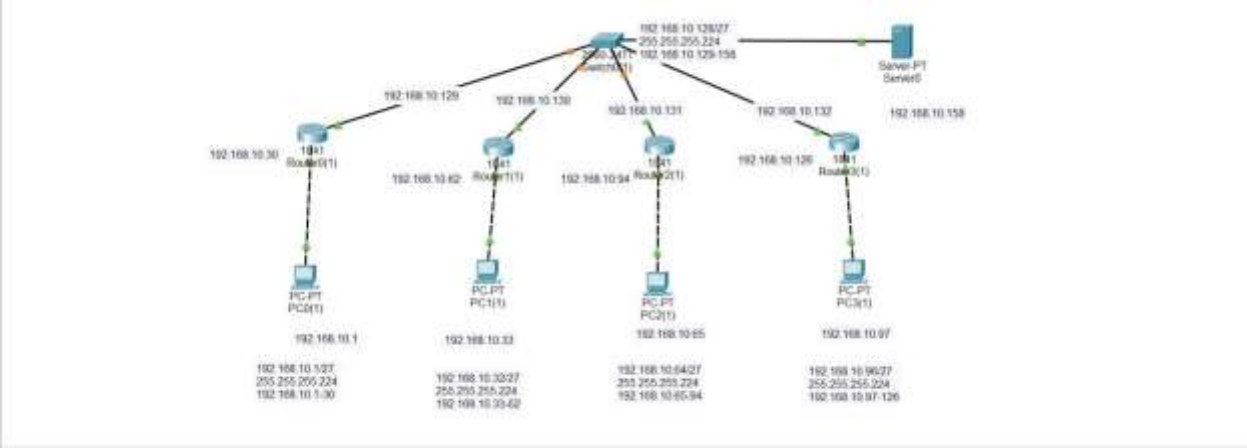
## 4. PROTOCOLO RIP (ROUTING INFORMATION PROTOCOL)

RIP es un protocolo de enrutamiento dinámico de tipo vector distancia. Utiliza el número de saltos (hop count) como métrica para determinar la mejor ruta hacia una red.

**Características principales de RIP:**

- Máximo de 15 saltos
- Actualización cada 30 segundos
- Fácil de configurar
- Adecuado para redes pequeñas

## 5. DESCRIPCIÓN DE LA TOPOLOGÍA




**La red utilizada en la simulación está compuesta por:**

- 4 Routers
- 1 Switch central
- 4 PCs
- 1 Servidor

**Se utiliza la red 192.168.10.0/24, dividida en subredes /27:**

- 192.168.10.0/27 → PC0 y Router0
- 192.168.10.32/27 → PC1 y Router1
- 192.168.10.64/27 → PC2 y Router2
- 192.168.10.96/27 → PC3 y Router3
- 192.168.10.128/27 → Red troncal (Switch y servidores)

## 6. DIRECCIONAMIENTO IP DE LA RED

**PCs**

- PC0: 192.168.10.1 Gateway: 192.168.10.30
- PC1: 192.168.10.33 Gateway: 192.168.10.62
- PC2: 192.168.10.65 Gateway: 192.168.10.94
- PC3: 192.168.10.97 Gateway: 192.168.10.126

**Routers (Interfaz LAN)**

- Router0: 192.168.10.30
- Router1: 192.168.10.62
- Router2: 192.168.10.94
- Router3: 192.168.10.126

**Routers (Hacia Switch Troncal)**

- Router0: 192.168.10.129
- Router1: 192.168.10.130
- Router2: 192.168.10.131
- Router3: 192.168.10.132

**Servidor**

- Server0: 192.168.10.158

## 7. CONFIGURACIÓN DE RIP EN CISCO PACKET TRACER

La configuración se realiza en cada router desde la línea de comandos (CLI).

7.1 Configuración en Router0

```
enable
configure terminal
router rip
version 2
network 192.168.10.0
no auto-summary
```

7.2 Configuración en Router1

```
enable
configure terminal
router rip
version 2
```

network 192.168.10.0

no auto-summary

7.3 Configuración en Router2

enable

configure terminal

router rip

version 2

network 192.168.10.0

no auto-summary

7.4 Configuración en Router3

enable

configure terminal

router rip

version 2

network 192.168.10.0

no auto-summary

## 8. FUNCIONAMIENTO DE RIP EN LA TOPOLOGÍA

Una vez activado RIP en todos los routers, estos comienzan a intercambiar información automáticamente sobre sus redes. Cada router aprende las rutas hacia las demás subredes sin necesidad de configurarlas manualmente.

Gracias a esto, todas las PCs pueden comunicarse entre sí y también con el servidor ubicado en la red troncal.

## 9. VERIFICACIÓN DE CONECTIVIDAD

Para comprobar el correcto funcionamiento del enrutamiento dinámico con RIP se utilizan los siguientes comandos:

**Desde las PCs**

ping 192.168.10.33

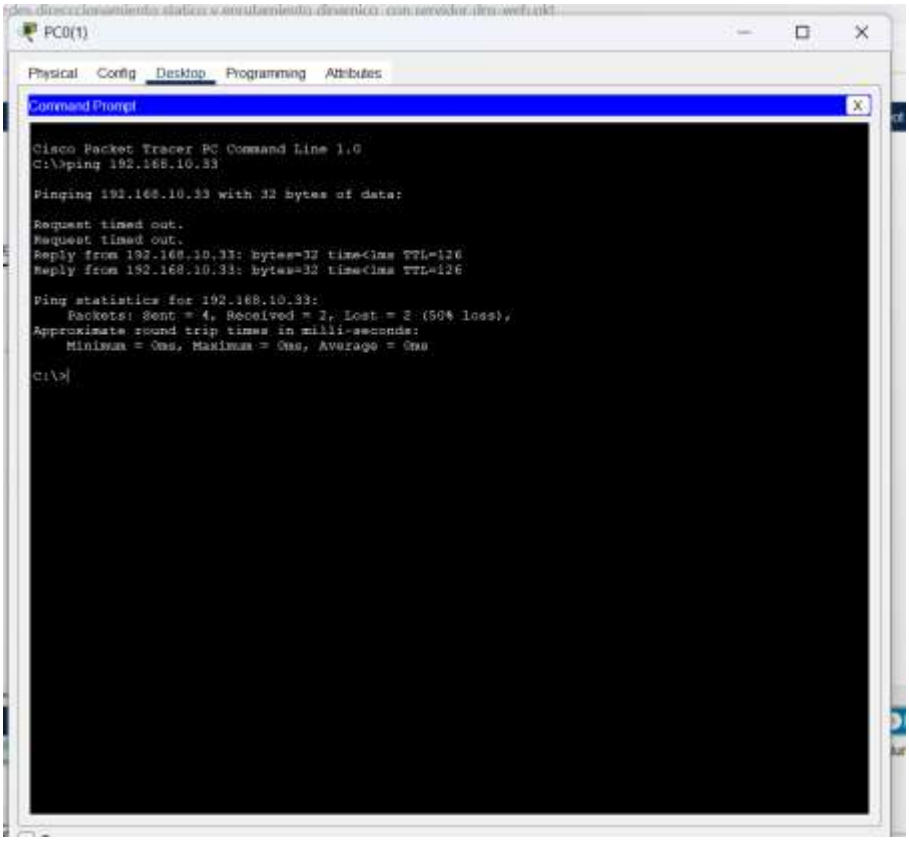
ping 192.168.10.65

ping 192.168.10.97

ping 192.168.10.158

Desde los routers

show ip route




Si las rutas RIP aparecen con la letra R, significa que el protocolo está funcionando correctamente a veces el primero paquete se pierden pero ya después hacerlo otra ves ya envía directo**.**

## 10. VENTAJAS Y DESVENTAJAS DE RIP

### Ventajas

- Fácil configuración
- Aprendizaje automático de rutas
- Ideal para redes pequeñas

### Desventajas

- Límite de 15 saltos
- Convergencia lenta
- No es adecuado para redes grandes

## 11. CONCLUSIÓN

El enrutamiento dinámico permite que las redes funcionen de manera más eficiente y automática. El protocolo RIP, aunque es sencillo, resulta muy útil para fines educativos y redes pequeñas.

Mediante la simulación en Cisco Packet Tracer fue posible comprobar cómo los routers intercambian información de forma automática, permitiendo la comunicación entre todas las subredes y el servidor sin necesidad de configurar rutas individuales en cada equipo.

# VLANS Y CONFIGURACIÓN DE SWITCHES

## 1. INTRODUCCIÓN

Las redes de computadoras actuales requieren una adecuada organización para mejorar el rendimiento, la seguridad y la administración de los equipos. Una de las técnicas más utilizadas para lograr esto es el uso de VLANs (Virtual Local Area Networks).

Una VLAN permite dividir una red física en varias redes lógicas, sin necesidad de usar switches físicos adicionales. En este reporte se explica el concepto de VLANs y la configuración de switches, utilizando una simulación en Cisco Packet Tracer para PC, basada en la topología proporcionada.

## 2. ¿QUÉ ES UNA VLAN?

Una VLAN es una red virtual que agrupa dispositivos dentro de un mismo switch o entre varios switches, aunque estén físicamente en diferentes lugares. Los equipos dentro de una misma VLAN pueden comunicarse entre sí como si estuvieran en la misma red física.

Las VLANs se utilizan para:

- Mejorar la seguridad
- Reducir el tráfico innecesario
- Facilitar la administración de la red
- Separar departamentos o áreas de trabajo

## 3. VENTAJAS DEL USO DE VLANs

- Mayor seguridad de la información
- Mejor desempeño de la red
- Organización por departamentos
- Reducción de dominios de broadcast
- Fácil administración

## 4. DESCRIPCIÓN DE LA TOPOLOGÍA (SEGÚN LA IMAGEN)

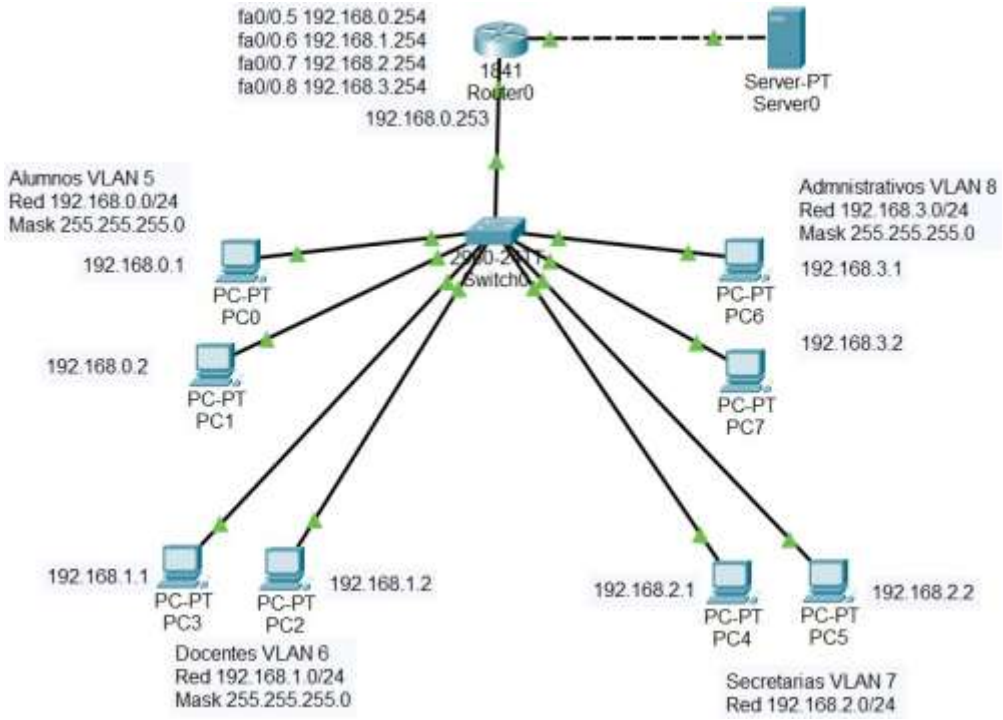
La red simulada está compuesta por:

- 1 Router Cisco 1841
- 1 Switch Cisco 2960
- 8 Computadoras (PCs)
- 1 Servidor

La red está dividida en cuatro VLANs:

- **VLAN 5 – Alumnos**
  - Red: 192.168.0.0/24
  - PC0: 192.168.0.1
  - PC1: 192.168.0.2
- **VLAN 6 – Docentes**
  - Red: 192.168.1.0/24
  - PC3: 192.168.1.1
  - PC2: 192.168.1.2
- **VLAN 7 – Secretarias**
  - Red: 192.168.2.0/24
  - PC4: 192.168.2.1
  - PC5: 192.168.2.2
- **VLAN 8 – Administrativos**
  - Red: 192.168.3.0/24
  - PC6: 192.168.3.1
  - PC7: 192.168.3.2

El router se conecta al switch mediante un enlace troncal para permitir el enrutamiento entre VLANs.




**5. CONFIGURACIÓN DE LAS VLANs EN EL SWITCH**

Primero se crean las VLANs:

enable

configure terminal

vlan 5

name ALUMNOS

vlan 6

name DOCENTES

vlan 7

name SECRETARIAS

vlan 8

name ADMINISTRATIVOS

exit

## 6. ASIGNACIÓN DE PUERTOS A LAS VLANs

Ejemplo de asignación de puertos:

interface range fa0/1 - 2

switchport mode access

switchport access vlan 5

interface range fa0/3 - 4

switchport mode access

switchport access vlan 6

interface range fa0/5 - 6

switchport mode access

switchport access vlan 7

interface range fa0/7 - 8

switchport mode access

switchport access vlan 8

```
Switch>show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gig0/1, Gig0/2
5    Alumnos                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6
6    docentes                         active    Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12
7    Secretarias                      active    Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18
8    Administrativos                  active    Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Switch>
```

## 7. CONFIGURACIÓN DEL ENLACE TRONCAL (TRUNK)

El enlace entre el switch y el router se configura como troncal para transportar todas las VLANs:

interface fa0/24

switchport mode trunk

## 8. CONFIGURACIÓN DEL ROUTER (ROUTER-ON-A-STICK)

El router permite la comunicación entre las VLANs mediante subinterfaces:

interface fa0/0.5

encapsulation dot1Q 5

ip address 192.168.0.254 255.255.255.0

interface fa0/0.6

encapsulation dot1Q 6

ip address 192.168.1.254 255.255.255.0

interface fa0/0.7

encapsulation dot1Q 7

ip address 192.168.2.254 255.255.255.0

interface fa0/0.8

encapsulation dot1Q 8

ip address 192.168.3.254 255.255.255.0

## 9. CONFIGURACIÓN DE LAS PCs

Cada PC se configura con:

- Dirección IP correspondiente a su VLAN
- Máscara 255.255.255.0
- Puerta de enlace igual a la IP del router de su VLAN

Ejemplo para VLAN 5:

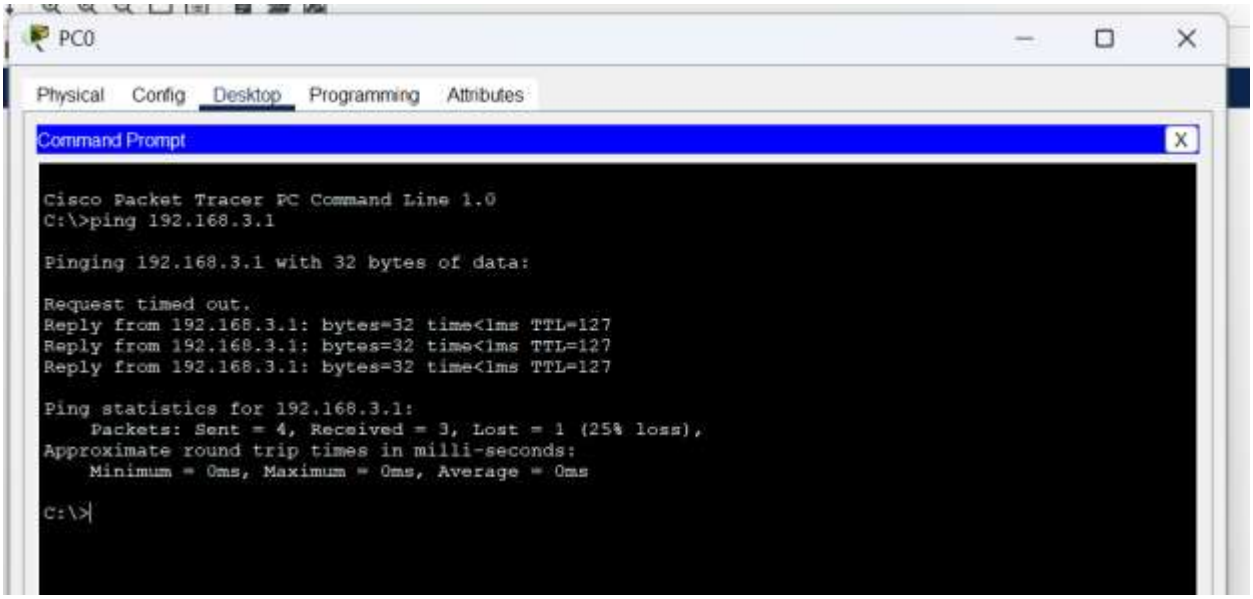
- PC0: 192.168.0.1 / Gateway 192.168.0.254
- PC1: 192.168.0.2 / Gateway 192.168.0.254

## 10. VERIFICACIÓN DE CONECTIVIDAD

Se realizan pruebas de conectividad usando el comando:

ping 192.168.3.1

ping 192.168.2.1




Si todas las VLANs fueron configuradas correctamente, las PCs podrán comunicarse entre sí a través del router.

## 11. CONCLUSIÓN

Las VLANs permiten organizar una red de manera eficiente, segura y ordenada. En esta simulación realizada en Cisco Packet Tracer se logró dividir la red en cuatro VLANs correspondientes a diferentes áreas de trabajo.

La correcta configuración del switch y del router permitió que los equipos de distintas VLANs pudieran comunicarse entre sí de forma segura mediante el enrutamiento inter-VLAN.

# SIMULACIÓN DE UNA RED LAN

## 1. INTRODUCCIÓN

Las redes de área local (LAN) permiten la comunicación entre computadoras y dispositivos dentro de un mismo espacio físico, como un salón de clases, una oficina o un edificio. La simulación de una red LAN es una práctica fundamental para comprender cómo funcionan las conexiones, las direcciones IP, la comunicación de datos y los servicios de red.

## 2. ¿QUÉ ES UNA RED LAN?

Una Red de Área Local (LAN) es una red que conecta varios dispositivos dentro de un área pequeña, como una casa, una escuela o una empresa. Sus principales características son:

- Alta velocidad de transmisión
- Bajo costo de instalación
- Uso de cableado o conexión inalámbrica
- Permite compartir recursos como archivos, impresoras e Internet

## 3. ¿QUÉ ES LA SIMULACIÓN DE UNA RED?

La simulación de una red consiste en crear un modelo virtual de una red real en un programa de computadora. Esto permite:

- Probar configuraciones
- Detectar errores
- Aprender sin riesgos
- Evitar daños en equipos reales

Cisco Packet Tracer es una herramienta que permite simular redes con routers, switches, computadoras y servidores de manera gráfica e interactiva.

## 4. ELEMENTOS UTILIZADOS EN LA SIMULACIÓN

Para la simulación de una red LAN se utilizan los siguientes dispositivos:

- Computadoras (PC)
- Switch
- Router
- Cables de red
- Software de simulación (Cisco Packet Tracer)

Cada uno cumple una función específica dentro de la red.

## 5. TOPOLOGÍA DE LA RED LAN

La topología empleada en la simulación es la topología en estrella, donde todas las computadoras se conectan a un switch central.

Ventajas de esta topología:

- Fácil mantenimiento
- Mayor estabilidad
- Si una computadora falla, la red sigue funcionando
- Mejor control del tráfico

## 6. DISEÑO DE LA RED A SIMULAR

Se diseña una red LAN para un salón de clases con los siguientes elementos:

- 1 Router
- 1 Switch
- 3 Computadoras

Direcciones de la red:

- Red: 192.168.1.0
- Máscara: 255.255.255.0
- Router: 192.168.1.1
- PC1: 192.168.1.2
- PC2: 192.168.1.3
- PC3: 192.168.1.4

## 7. CONFIGURACIÓN DEL ROUTER EN LA SIMULACIÓN

En Cisco Packet Tracer la configuración del router se realiza mediante comandos.

Router> enable

Router# configure terminal

Router(config)# interface g0/0

Router(config-if)# ip address 192.168.1.1 255.255.255.0

Router(config-if)# no shutdown

Esto permite que el router funcione como puerta de enlace de la red.

## 8. CONFIGURACIÓN DE LAS COMPUTADORAS

Cada computadora se configura con los siguientes datos:

PC1:

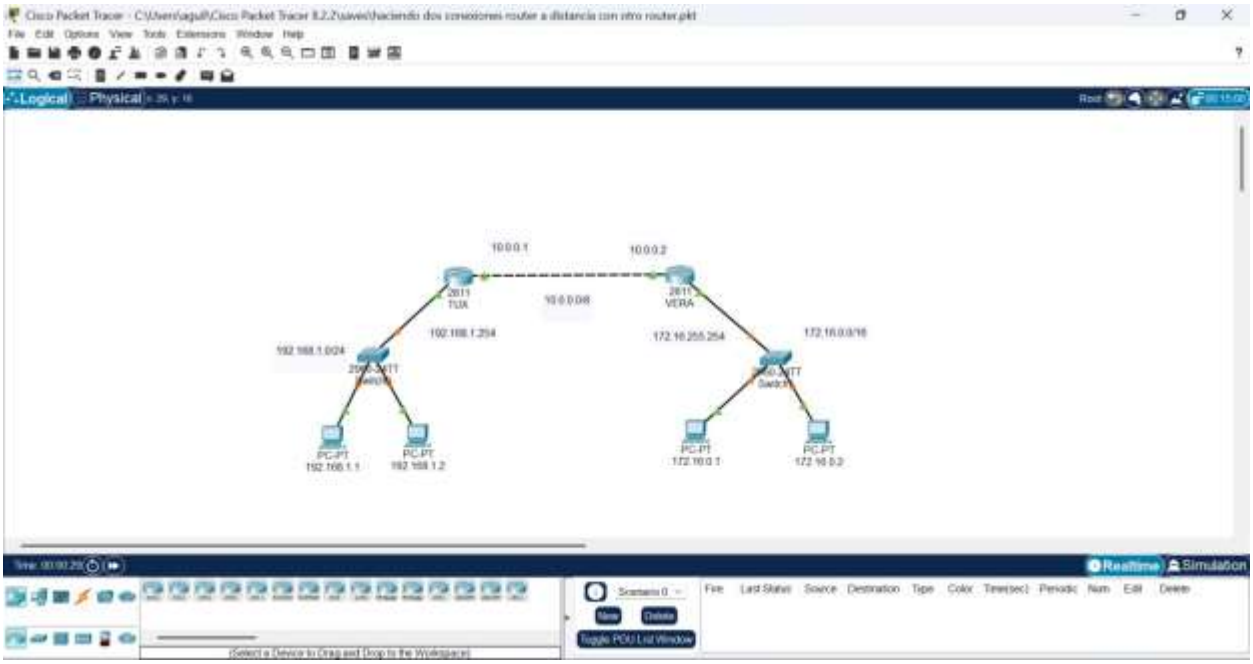
- IP: 192.168.1.2
- Máscara: 255.255.255.0
- Gateway: 192.168.1.1

PC2:

- IP: 192.168.1.3
- Máscara: 255.255.255.0
- Gateway: 192.168.1.1

PC3:

- IP: 192.168.1.4
- Máscara: 255.255.255.0
- Gateway: 192.168.1.1




**9.** VENTAJAS DE LA SIMULACIÓN DE UNA RED LAN
• Permite adquirir conocimientos sin necesidad de utilizar equipos reales
• Previene daños en dispositivos físicos
• Facilita la realización de prácticas y ejercicios
• Contribuye a la detección y corrección de errores
• Disminuye los costos de implementación

10. APLICACIÓN DE LA SIMULACIÓN EN LA VIDA REAL

La simulación de redes LAN se emplea en distintas situaciones, tales como:

• Capacitación y formación de estudiantes
• Planeación y diseño de redes empresariales
• Pruebas previas antes de una instalación real
• Análisis y solución de problemas de red

11. CONCLUSIÓN

La simulación de una red LAN es una herramienta esencial para el aprendizaje de redes de computadoras. A través del uso de Cisco Packet Tracer en una computadora es posible diseñar, configurar y comprobar redes de manera segura y eficaz.

Este tipo de prácticas facilita la comprensión del funcionamiento de los dispositivos de red, el manejo de direcciones IP y la comunicación entre equipos, fortaleciendo los conocimientos en el área de informática y telecomunicaciones.

DISEÑO Y SIMULACIÓN DE UNA RED INALÁMBRICA CON DHCP Y SEGURIDAD WiFi EN CISCO PACKET TRACER
1. INTRODUCCIÓN

Las redes inalámbricas hacen posible la comunicación entre dispositivos sin necesidad de cables físicos, utilizando ondas de radio mediante el estándar WiFi (IEEE 802.11). Su uso

es indispensable en instituciones educativas, empresas y hogares, ya que permiten la movilidad de los usuarios y reducen los costos de cableado.

En esta práctica se diseñó y simuló una red inalámbrica utilizando Cisco Packet Tracer, integrando routers, puntos de acceso inalámbricos (WRT300N), un switch, un servidor DHCP y dispositivos finales. Además, se aplicaron esquemas de direccionamiento IP, asignación automática de direcciones y mecanismos de seguridad.

## 2. OBJETIVO GENERAL

Diseñar, configurar y evaluar el funcionamiento de una red inalámbrica con asignación dinámica de direcciones IP mediante DHCP y con seguridad WiFi, utilizando Cisco Packet Tracer como herramienta de simulación.

### Objetivos específicos

- Configurar una red LAN tanto cableada como inalámbrica
- Implementar un servidor DHCP para la asignación automática de direcciones IP
- Configurar puntos de acceso inalámbricos
- Aplicar medidas de seguridad en la red WiFi
- Comprobar la conectividad entre los dispositivos de la red

## 3. MARCO TEÓRICO

### 3.1 Red Inalámbrica (Wireless LAN – WLAN)

Una WLAN es una red local que permite la comunicación entre dispositivos mediante ondas de radio. Utiliza puntos de acceso (Access Point) que conectan a los equipos inalámbricos con la red cableada principal.

### 3.2 DHCP (Dynamic Host Configuration Protocol)

DHCP es un protocolo de red encargado de asignar automáticamente a los dispositivos los siguientes parámetros:

- Dirección IP
- Máscara de subred
- Puerta de enlace (Gateway)
- Servidor DNS

El uso de DHCP elimina la necesidad de configurar manualmente cada equipo y reduce errores de configuración.

### 3.3 Seguridad en Redes WiFi

La seguridad en redes inalámbricas tiene como objetivo proteger el acceso a la red y evitar conexiones no autorizadas. Entre los métodos más utilizados se encuentran:

- WEP (obsoleto)
- WPA
- WPA2 (uno de los más utilizados)
- Filtrado por direcciones MAC

• Ocultamiento de SSID

4. DESCRIPCIÓN DE LA TOPOLOGÍA IMPLEMENTADA

La red simulada está conformada por los siguientes dispositivos:

• 1 Router principal (Router0)
• 1 Switch 2960
• 1 Servidor DHCP
• 3 Routers inalámbricos WRT300N
• 3 Computadoras de escritorio
• 3 Laptops

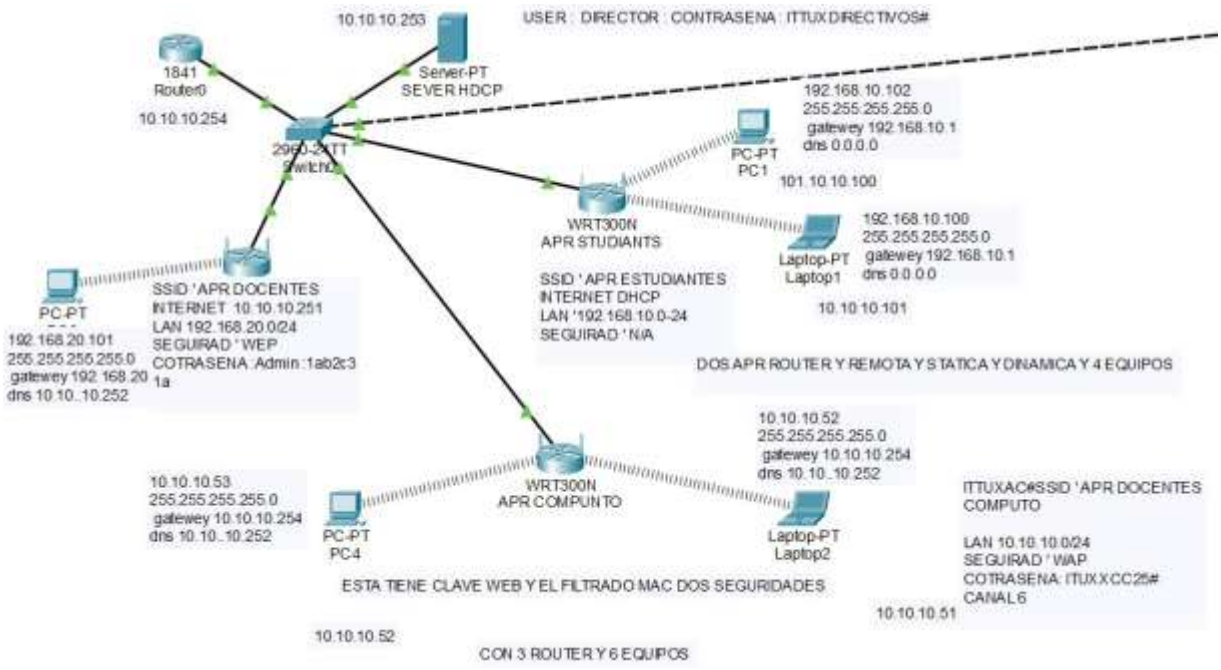
Redes utilizadas:

• Red 10.10.10.0 /24 → Interconexión principal
• Red 192.168.10.0 /24 → Red inalámbrica de estudiantes
• Red 192.168.20.0 /24 → Red inalámbrica de docentes

Cada router inalámbrico proporciona acceso a una red WiFi distinta, lo que permite segmentar a los usuarios y aplicar un mejor control de seguridad.

Topología en Cisco Packet Tracer, donde se visualizan:

• Router Cisco 1841
• Switch Cisco 2960
• Servidor
• Routers inalámbricos WRT300N
• Computadoras y laptops conectadas de forma inalámbricaUbicación exacta en el **reporte:**




**1. CONFIGURACIÓN DEL SERVIDOR DHCP (DESCRIPCIÓN TÉCNICA)**

El servidor DHCP se configuró con los siguientes parámetros:

- Dirección del servidor: **10.10.10.253**
- Gateway: **10.10.10.254**
- DNS: **10.10.10.252**
- Rango de IP asignadas:

**• Rango de direcciones asignadas: 192.168.10.100 – 192.168.10.200**

**• Máscara de subred: 255.255.255.0**

---

**FUNCIONAMIENTO DEL DHCP**

**El protocolo DHCP funciona mediante un proceso de intercambio de mensajes entre el cliente y el servidor para asignar automáticamente los parámetros de red:**

**El dispositivo cliente envía un mensaje denominado DHCP Discover solicitando una dirección IP.**

**El servidor responde con un DHCP Offer, ofreciendo una configuración disponible.**

**El cliente acepta la oferta mediante un mensaje DHCP Request.**

**Finalmente, el servidor confirma la asignación con un mensaje DHCP Acknowledgment (ACK).**

**Gracias a este proceso, computadoras y laptops obtienen su configuración de red de manera automática, sin necesidad de realizar ajustes manuales.**

---

**6. CONFIGURACIÓN DE LOS ROUTERS INALÁMBRICOS (WRT300N)**

**Router APR Estudiantes**

**• SSID: APR_ESTUDIANTES**

**• Red LAN: 192.168.10.0 /24**

**• Tipo de asignación IP: DHCP**

**• Seguridad: Sin cifrado (acceso abierto para estudiantes)**

---

**Router APR Docentes**

**• SSID: APR_DOCENTES**

**• Seguridad: WPA**

**• Contraseña: 1ab2c3**

**• Servidor DNS: 10.10.10.252**

**• Puerta de enlace: 192.168.20.1**

---

**Router APR Cómputo**

**• SSID: APR_COMPUTO**

**• Seguridad: WPA**

**• Contraseña: ITUXCC25#**

**• Filtrado por MAC: Activado**

**• Canal inalámbrico: 6**

---

## 7. SEGURIDAD EN LA RED WI-FI (DESCRIPCIÓN TÉCNICA)

**Para proteger la red inalámbrica se implementaron los siguientes mecanismos de seguridad:**

**a) Autenticación WPA**

**Este método emplea cifrado dinámico mediante claves compartidas, lo que impide el acceso de usuarios no autorizados a la red inalámbrica.**

**b) Filtrado por direcciones MAC**

**Solo se permite la conexión de dispositivos cuyas direcciones físicas estén previamente registradas en el router, incrementando el control de acceso.**

**c) Control de acceso por SSID**

**Cada red inalámbrica utiliza un identificador distinto, lo que permite:**

**• Separar a los usuarios por tipo de acceso**

**• Aplicar diferentes políticas de seguridad**

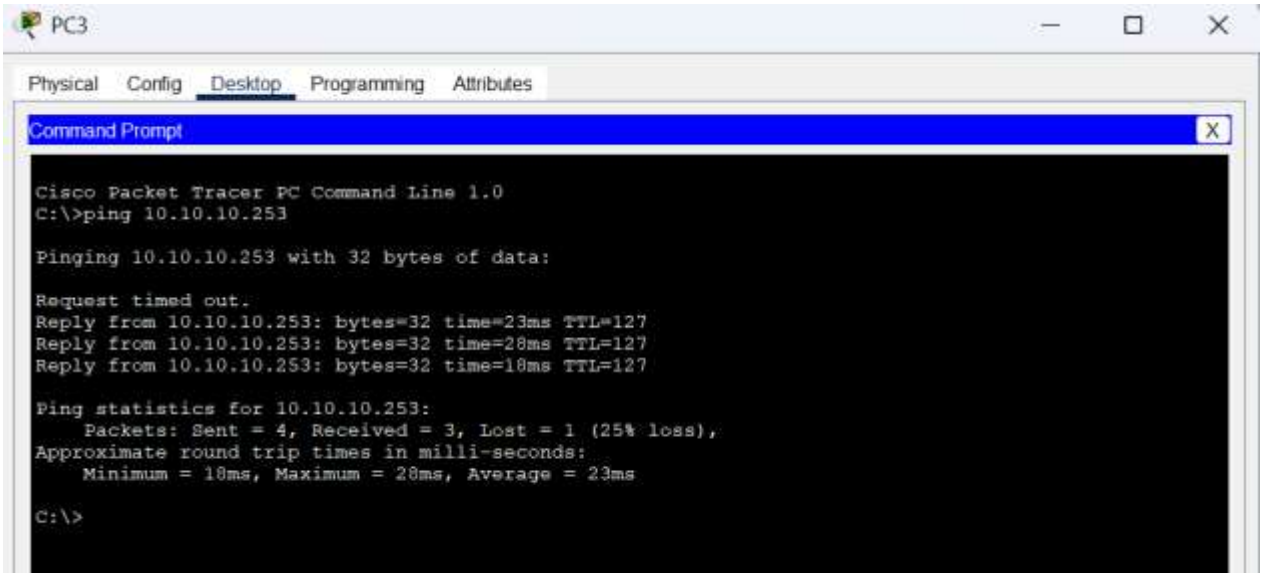
**• Controlar el tráfico dentro de la red**

**Estas medidas fortalecen la protección contra accesos no autorizados y garantizan la confidencialidad de la información transmitida .**

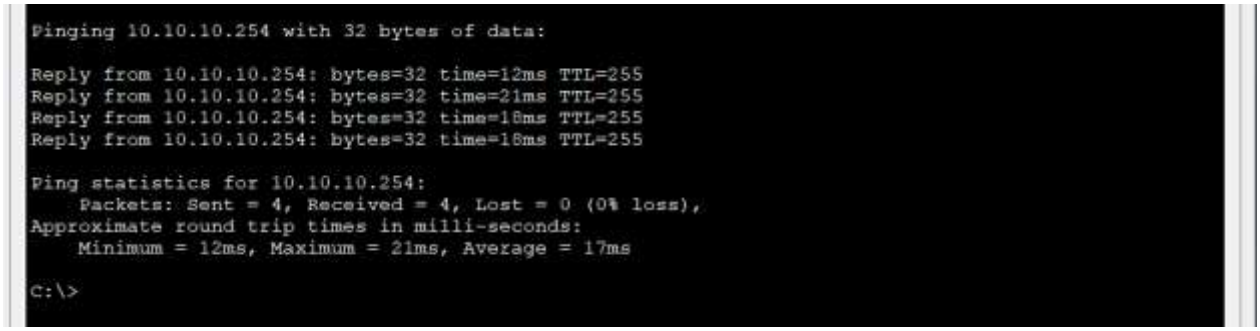
## 2. VERIFICACIÓN DE CONECTIVIDAD

Se realizaron pruebas de conexión mediante:

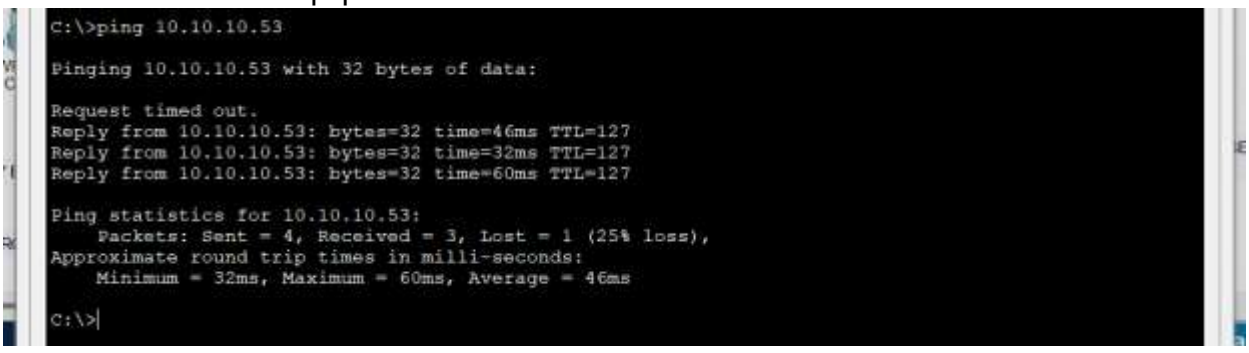
- Comandos **ping** desde las PCs a:
    - Servidor:




    - Gateway:




    - Otros equipos de la red:



Los resultados fueron satisfactorios, comprobando que:

- El DHCP funciona correctamente
- Los equipos se comunican entre sí
- El acceso a la red es estable

## 3. CONCLUSIÓN

La práctica permitió comprender de forma clara el funcionamiento de las redes inalámbricas, el uso del protocolo DHCP y la importancia de la seguridad WiFi. Mediante Cisco Packet Tracer se logró una simulación realista de una red escolar con múltiples routers inalámbricos y segmentación de usuarios.

El uso de seguridad como WPA y filtrado MAC garantiza que solo los usuarios autorizados tengan acceso a la red, evitando riesgos de ataques y robo de información.