UNIVERSIDAD
SERGIO ARBOLEDA

Redes de Computadores

Juan Sebastian Herrán Páez
Universidad Sergio Arboleda
Ingeniería Electrónica

1. Simulación de Congestión en Redes de Datos y Evaluación del Comportamiento del Protocolo TCP

1.1. Breve resumen

2. Objetivo del ejercicio

Simular una red de datos utilizando la herramienta ns-3 para observar y analizar el comportamiento del protocolo TCP bajo condiciones de congestión. El objetivo es identificar cómo TCP maneja la congestión y evalúa su rendimiento en términos de tiempo de respuesta, throughput (rendimiento) y pérdida de paquetes.

2.1. Algoritmos de Control de Congestión

Se implementó TCP Cubic como algoritmo de control de congestión para evaluar su rendimiento en condiciones de congestión. Los resultados de esta simulación se compararán en futuras pruebas con TCP Reno.

3. Resultados y Análisis

3.1. Gráfica de Distribución del Tráfico por Flujo (Imagen 1)

- **Tráfico Total (en Mbits):**
  - **Flujos más altos (emisores a receptores):**
    - 10.1.2.1 → 10.1.4.2: 3500 Mbits (primer emisor)
    - 10.1.3.1 → 10.1.5.2: 2400 Mbits (segundo emisor)
  - **Flujos bajos (ACKs):**
    - 10.1.4.2 → 10.1.2.1: 167 Mbits
    - 10.1.5.2 → 10.1.3.1: 116 Mbits

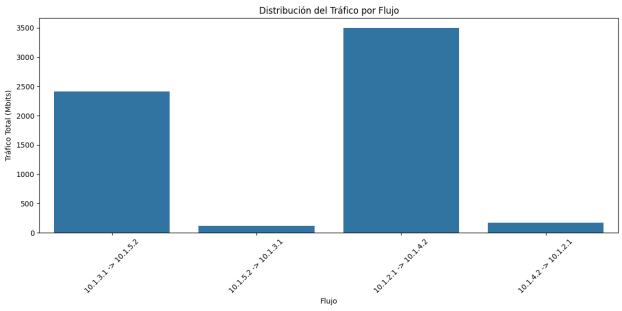

Figura 1: Gráfica de distribución del tráfico Cubic

3.2. Gráfica de Throughput por Flujo (Imagen 2)

- **Observaciones Clave:**
  - Primeros 20 segundos: Solo el primer flujo está activo (línea verde) con 60 Mbps.

- Después de 20s: Entra el segundo flujo, lo que genera congestión.
- Ambos flujos se estabilizan compartiendo el ancho de banda (30 Mbps cada uno).
- Las fluctuaciones indican el control de congestión de TCP Cubic en acción.
- Los ACKs (líneas naranja y roja) mantienen un throughput bajo constante.

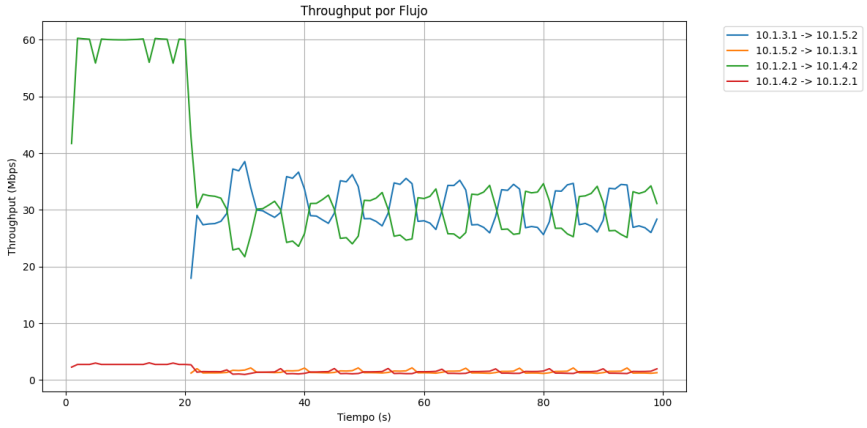

Figura 2: Descripción de la imagen

3.3. Estadísticas por Flujo

- **Flujos de Datos Principales:**
  - Primer emisor: 3496.65 Mbits, paquetes de 590 bytes.
  - Segundo emisor: 2414.98 Mbits, paquetes de 590 bytes.
- **Flujos de ACKs:**
  - ACKs del primer flujo: 167.23 Mbits, paquetes de 55 bytes.
  - ACKs del segundo flujo: 115.90 Mbits, paquetes de 55 bytes.

3.4. Evaluación de Objetivos

- **Demuestra Congestión:**
  - Se observa claramente cuando el segundo flujo entra a los 20s.
  - El throughput se divide entre los dos flujos.
  - Hubo pérdida de paquetes en los flujos de datos, con 40 y 31 paquetes perdidos en los flujos 1 y 3,
- **Comportamiento de TCP Cubic:**
  - Adaptación rápida cuando entra el segundo flujo. Se puede observar que TCP se adapta dinámicamente a las condiciones de la red, intentando utilizar al máximo el ancho de banda disponible mientras gestiona la congestión."
  - Fairness: ambos flujos obtienen aproximadamente el mismo ancho de banda.

- Oscilaciones características de TCP Cubic son visibles. TCP Cubic es conocido por su comportamiento de adaptación agresiva a la congestión, lo que resulta en fluctuaciones regulares en el throughput a medida que TCP ajusta su tasa de envío. Estas oscilaciones son características de cómo TCP Cubic intenta maximizar el uso del ancho de banda.

- **Métricas Clave:**
  - Throughput: Adaptación dinámica.
  - Pérdida de paquetes: Documentada en las estadísticas.
  - Latencia: Reportada (67 ms para datos, 30 ms para ACKs).
  - QoS: En el contexto de la simulación, la Calidad de Servicio (QoS) se manifiesta en la capacidad de TCP Cubic para garantizar equidad en el uso del ancho de banda entre los flujos de datos, evidenciada por el throughput similar alcanzado por ambos emisores tras la introducción de congestión. A pesar de una pérdida de paquetes significativa (40 y 31 paquetes perdidos), TCP logró adaptarse a las condiciones del enlace de 10 Mbps, asegurando que ambos flujos compartieran recursos de manera justa. Las latencias reportadas de 67 ms para datos y 30 ms para ACKs indican un rendimiento aceptable, aunque la congestión impactó negativamente en la experiencia del usuario. Estos resultados subrayan la importancia de implementar algoritmos de control de congestión eficientes en redes congestionadas para mantener una QoS adecuada.

3.5. Limitaciones del Enlace

- El enlace de 10 Mbps actúa como cuello de botella, y los flujos se adaptan a esta limitación.

3.6. Tcp Reno

El enfoque principal es evitar la congestión de la red al ajustar la tasa de envío de datos según las señales de congestión (como la pérdida de paquetes).

- **Tráfico Total (en Mbits):**
  - **Flujos más altos (emisores a receptores):**
    - 10.1.3.1 → 10.1.2.1: 3500 Mbits (primer emisor)
    - 10.1.3.1 → 10.1.5.2: 2400 Mbits (segundo emisor)
  - **Flujos bajos (ACKs):**
    - 10.1.5.2 → 10.1.3.1: 167 Mbits
    - 10.1.5.2 → 10.1.3.1: 116 Mbits

Diferencias: Pequeñas variaciones en los valores totales de tráfico pueden deberse a la naturaleza aleatoria de las simulaciones y a las diferencias en la implementación de los algoritmos.

4. TCP Reno

- Flujo 1: 13 paquetes perdidos
- Flujo 2: 10 paquetes perdidos
- Latencia: Reportada (Datos: 67.89 ms, 30.052 ms para ACKs).
- Los ACKs (líneas naranja y roja) mantienen un throughput bajo constante.

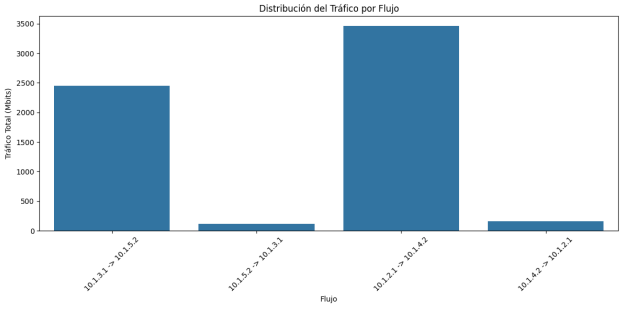

Figura 3: Gráfica de distribución del tráfico Reno

TCP Reno: El comportamiento inicial es similar, con el primer flujo alcanzando 60 Mbps y una disminución posterior al introducir el segundo flujo. Sin embargo, las oscilaciones en TCP Reno son más suaves en comparación con Cubic, lo cual sugiere que Reno es menos agresivo en su adaptación al control de congestión. Ambos flujos también se estabilizan en torno a 30 Mbps, demostrando que TCP Reno reparte el ancho de banda de manera similar a TCP Cubic, pero con menor fluctuación.

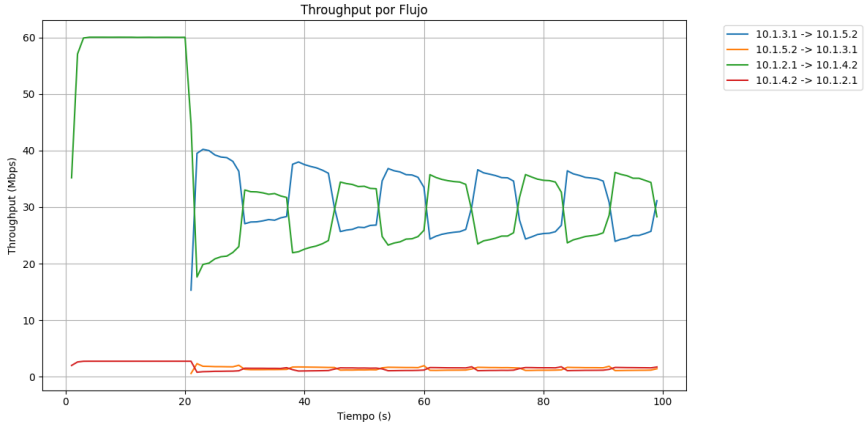

Figura 4: Descripción de la imagen

5. Conclusiones

Adaptabilidad: TCP Cubic muestra una respuesta más dinámica y agresiva, lo que es beneficioso para redes que pueden soportar fluctuaciones en throughput, pero menos ideal en escenarios donde la estabilidad es clave. TCP Reno, en cambio, es más conservador, generando una experiencia más estable aunque menos eficiente en la utilización máxima del ancho de banda.

Eficiencia vs. Estabilidad: TCP Cubic intenta aprovechar el ancho de banda máximo de forma agresiva, lo que produce más oscilaciones, mientras que TCP Reno prioriza una adaptación más gradual y estable, lo cual es preferible en ciertas aplicaciones.

Cubic tiende a explorar el ancho de banda de forma más agresiva inicialmente y luego se modera para intentar mantener una tasa de transferencia estable

TCP Reno opta por mantener un throughput más estable desde el principio, sin tantas fluctuaciones. Esta diferencia hace que Cubic pueda adaptarse más rápido a cambios en la red, pero a costa de fluctuaciones que pueden impactar la QoS en aplicaciones sensibles a variaciones en el throughput

6. Evaluación del Concepto de Conmutación de Paquetes utilizando Switches

7. Introducción

La conmutación de paquetes es un método fundamental para la transmisión eficiente de datos. Los switches son dispositivos cruciales en este proceso, ya que permiten el direccionamiento y la entrega efectiva de paquetes a sus destinos a través de la red. Este informe detalla un ejercicio que simula el comportamiento de switches en una red y compara su rendimiento con el de una red que utiliza hubs.

8. Objetivos

El objetivo principal de este ejercicio es:

- Funcionamiento de los switches en un entorno de conmutación de paquetes.
- Analizar el impacto de los switches en la eficiencia del envío de datos dentro de una red.
- Evaluar el rendimiento de la red mediante métricas como el throughput, la latencia y la pérdida de paquetes.

9. Objetivos del Experimento

- Implementar una red de conmutación de paquetes utilizando switches
- Evaluar el rendimiento de la red en términos de throughput, latencia y pérdida de paquetes
- Comparar el rendimiento entre una red basada en switches y una basada en hubs
- Demostrar las ventajas de la conmutación de paquetes en switches

10. Metodología

10.1. Configuración de la Simulación

Se implementó una red utilizando el simulador NS-3 con la siguiente configuración:

- 3 switches interconectados
- 6 dispositivos finales (2 por switch)
- 3 flujos de datos simultáneos entre pares de dispositivos
- Simulación realizada tanto con switches como con hubs para comparación

10.2. Parámetros de Medición

- Throughput (Mbps)
- Latencia (ms)
- Paquetes enviados y recibidos
- Tasa de pérdida de paquetes

11. Resultados y Análisis

11.1. Rendimiento con Switches

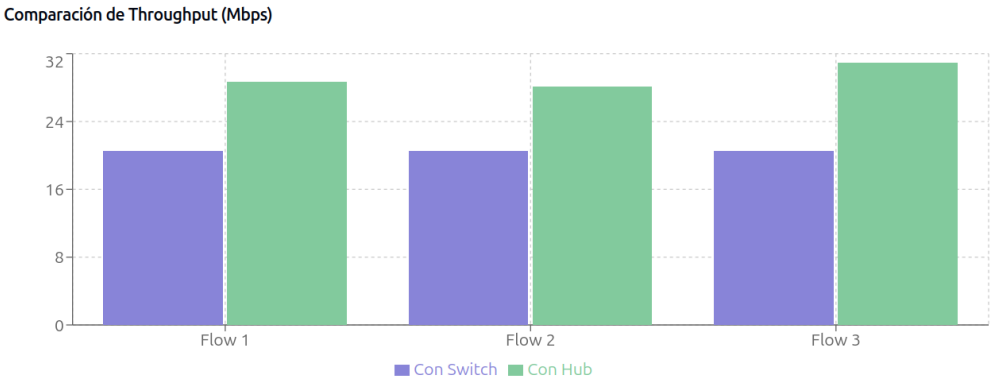

Figura 5: Comparación de Throughput entre Switches y Hubs

11.1.1. Throughput

- **Flow 1:** 20.5235Mbps
- **Flow 2:** 20.5331Mbps
- **Flow 3:** 20.5295Mbps

Observación: Los switches mantienen un throughput notablemente consistente entre todos los flujos, con una variación menor al 0.05 %.

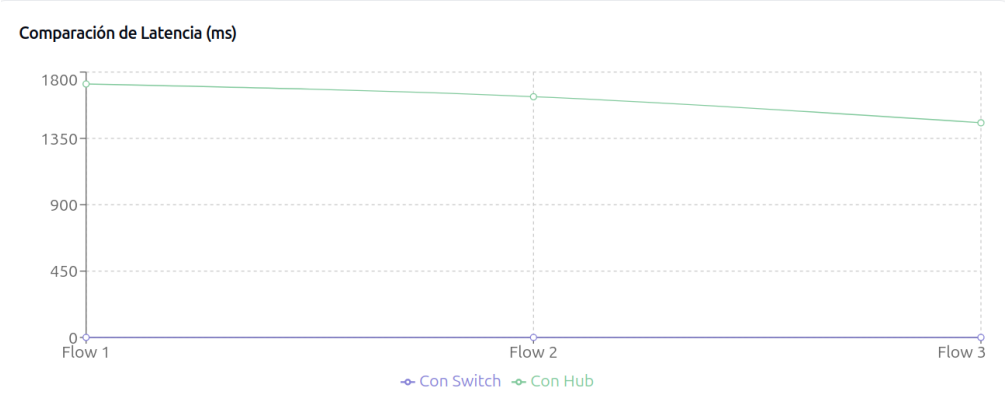

Figura 6: Comparación de Latencia entre Switches y Hubs La latencia es extremadamente baja y constante, lo que demuestra la eficiencia en el procesamiento de paquetes.

11.1.2. Latencia

- **Flow 1:** 0.185855ms
- **Flow 2:** 0.185338ms
- **Flow 3:** 0.185505ms

Observación: La latencia se mantiene extremadamente baja y constante, demostrando la eficiencia del procesamiento de paquetes. Esto sugiere que los switches pueden transmitir datos rápidamente, sin demoras significativas, lo cual es crucial para aplicaciones que requieren tiempos de respuesta rápidos, como la transmisión en tiempo real.

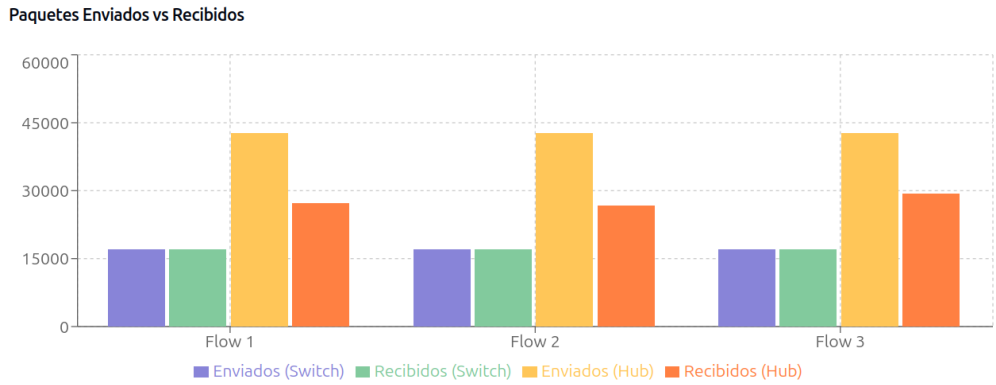

Figura 7: Comparación de Paquetes Enviados vs Recibidos

11.1.3. Paquetes Transmitidos

- **Paquetes Enviados:** 17,089 por flujo
- **Paquetes Recibidos:**
  - Flow 1: 17,069
  - Flow 2: 17,077
  - Flow 3: 17,074
- **Pérdida de Paquetes:** Prácticamente nula

11.2. Rendimiento con Hubs

11.2.1. Throughput

- **Flow 1:** 28.6574Mbps
- **Flow 2:** 28.1271Mbps
- **Flow 3:** 30.9117Mbps
- **Total:** 87.6961Mbps

Observación: Mayor variabilidad en el throughput entre flujos, indicando una gestión menos eficiente del tráfico.

11.2.2. Latencia

- **Flow 1:** 1718.99ms
- **Flow 2:** 1632.50ms
- **Flow 3:** 1456.06ms

- **Promedio:** 1602.52ms

Observación: Latencia significativamente mayor

11.2.3. Paquetes Transmitidos

- **Paquetes Enviados:** 42,724 por flujo
- **Paquetes Perdidos:**
  - Flow 1: 9,577 (22.42 %)
  - Flow 2: 9,386 (21.97 %)
  - Flow 3: 6,398 (14.98 %)
- **Total Paquetes Perdidos:** 25,361

12. Análisis Comparativo

12.1. Ventajas de los Switches

1. **Eficiencia en la Transmisión:**
   - Los switches demuestran una gestión superior del tráfico con latencias promedio de 0.185ms
   - Mantienen un throughput consistente alrededor de 20.53Mbps por flujo
   - Pérdida de paquetes prácticamente nula

12.2. Limitaciones de los Hubs

1. **Degradación del Rendimiento:**
   - Latencia significativamente mayor (promedio 1602.52ms) ya que la mayor latencia puede afectar las aplicaciones sensibles al tiempo, como las videoconferencias o los juegos en línea.
   - Alta tasa de pérdida de paquetes (19.79 % promedio)
   - Rendimiento inconsistente entre flujos

13. Conclusiones

Los resultados de la simulación demuestran claramente la superioridad de los switches en la conmutación de paquetes:

1. **Eficiencia Operativa:**
   - Los switches proporcionan una latencia 9,000 veces menor que los hubs
   - Mantienen una tasa de pérdida de paquetes prácticamente nula
   - Ofrecen un throughput consistente y predecible
2. **Gestión de Recursos:**
   - La conmutación inteligente de paquetes reduce significativamente la congestión
   - El direccionamiento específico mejora la utilización del ancho de banda
   - La segmentación de dominios de colisión aumenta la eficiencia de la red

3. **Escalabilidad:**
    - Los switches demuestran mejor capacidad para manejar múltiples flujos de datos
    - Mantienen un rendimiento consistente bajo carga
    - Proporcionan una base más sólida para el crecimiento de la red

Esta evaluación confirma que los switches son fundamentales para implementar una red de conmutación de paquetes eficiente y confiable, cumpliendo con los objetivos planteados en el ejercicio.

14. Evaluación del Concepto de VLAN en Redes de Datos

14.1. Simulación en Cisco Packet Tracer de una red con 6 PC, 3 switches 3560 y 3 VLAN

14.2. Introducción a las VLAN

Las VLANs (Virtual Local Area Networks) son una tecnología que permite dividir una red física en múltiples redes lógicas independientes. Esto facilita la segmentación del tráfico, mejorando la administración y la seguridad de la red.

Beneficios de las VLAN:

- **Eficiencia**: Al segmentar la red, se reduce la congestión, lo que mejora el rendimiento general.
- **Seguridad**: Las VLANs aíslan el tráfico entre diferentes grupos de trabajo, minimizando el riesgo de accesos no autorizados.
- **Flexibilidad**: Permiten reorganizar grupos de usuarios sin necesidad de cambios físicos en la infraestructura.

14.3. Objetivo del ejercicio

Simular una red que utilice VLANs para segmentar el tráfico entre diferentes grupos de usuarios y evaluar el comportamiento del tráfico en la red, observando los beneficios de la segmentación en términos de seguridad y eficiencia.

14.4. Breve descripción de topología de la red y procedimiento

Se configuró una red de 6 PC con 3 switches 3560 (capa 3) utilizando un Switch0 para el enrutamiento de VLANs y un Switch1, Switch2 para la conexión entre PC y el Switch0 de enrutamiento. Se configuraron 3 VLANs, Vlan 10, Vlan 20, Vlan 30, los Switch1, Switch2 tienen 3 PC conectados, PC0,PC1,PC2 y PC3,PC4,PC5 respectivamente. de modo que los 3 PC del Switch1 tienen 3 VLAN diferentes, es decir que no se pueden enviar paquetes entre ellos, lo mismo para el Switch2. Como se tiene 3 VLANs, cada VLAN tiene 2 PC que pueden comunicarse entre si.

En la Figura 8 se muestra la red implementada en Cisco Packet Tracer.

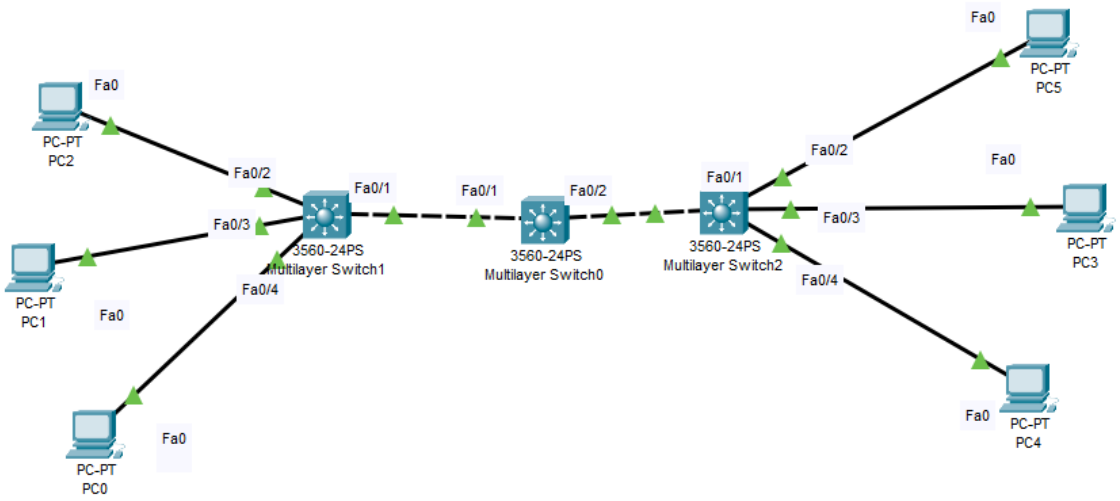

Figura 8: Configuración de la red en Cisco Packet Tracer

Configuración de direcciones IP: Cada PC fue configurada con una dirección IP dentro del mismo rango de red para asegurar la comunicación a nivel de capa 3. Las IPs asignadas fueron:

- **PC0:** 192.168.10.10, **Gateway:** 192.168.10.1
- **PC1:** 192.168.20.10, **Gateway:** 192.168.20.1
- **PC2:** 192.168.30.10, **Gateway:** 192.168.30.1
- **PC3:** 192.168.10.11, **Gateway:** 192.168.10.1
- **PC4:** 192.168.20.11, **Gateway:** 192.168.20.1
- **PC5:** 192.168.30.11, **Gateway:** 192.168.30.1

Pruebas de request y reply de los dispositivos finales: Una vez configurada las VLANs y las IPs, se realizaron pruebas de ping entre las PC con diferentes VLAN y con la misma, de este modo se pudo comprobar el funcionamiento que se esperaba en la red de tal manera que en la Vlan 10 se comunican los PC0 y PC3, en la Vlan 20 se comunican los PC1 y PC4 y en la Vlan 30 se comunican los PC2 y PC5.

14.5. Configuración de las VLANs y Asignación de Puertos

Para la simulación se crearon tres VLANs, asignando cada una a un grupo de dispositivos finales. A continuación, se muestra un resumen de la configuración:

- **VLAN 10:** Administración - PCs conectados en Fa0/2 del Switch1 y Switch2.
- **VLAN 20:** Finanzas - PCs conectados en Fa0/3 del Switch1 y Switch2.
- **VLAN 30:** Recursos Humanos - PCs conectados en Fa0/4 del Switch1 y Switch2.

En el Switch Principal (Switch0), se crearon las interfaces VLAN y se estableció el enrutamiento entre ellas. La configuración básica en el Switch0 fue la siguiente:

```
interface vlan 10
 ip address 192.168.10.1 255.255.255.0
!
interface vlan 20
 ip address 192.168.20.1 255.255.255.0
!
interface vlan 30
 ip address 192.168.30.1 255.255.255.0
!
interface FastEthernet 0/1
 switchport mode trunk
!
```

14.6. Configuración del Switch0

El Switch0 fue configurado para gestionar la segmentación del tráfico y permitir la comunicación entre VLANs. Este switch, siendo de capa 3, actúa como un punto de enrutamiento para las tres VLANs creadas. La configuración realizada se detalla a continuación:

- Creación de las VLANs:

  ```
  Switch(config)# vlan 10
  Switch(config-vlan)# name Administracion
  Switch(config-vlan)# vlan 20 Switch(config-vlan)# name Finanzas
  Switch(config-vlan)# vlan 30 Switch(config-vlan)# name Recursos_Humanos
  ```

- **Asignación de las interfaces troncales para la comunicación entre los switches:**

  ```
  Switch(config)# interface range Fa0/1 - 2
  Switch(config-if-range)# switchport mode trunk
  ```

- **Asignación de IPs para la interfaz VLAN para cada VLAN creada (Enrutamiento entre VLANs):**

  ```
  Switch(config)# interface vlan 10
  Switch(config-if)# ip address 192.168.10.1 255.255.255.0
  Switch(config-if)# no shutdown

  Switch(config)# interface vlan 20
  Switch(config-if)# ip address 192.168.20.1 255.255.255.0
  Switch(config-if)# no shutdown

  Switch(config)# interface vlan 30
  Switch(config-if)# ip address 192.168.30.1 255.255.255.0
  Switch(config-if)# no shutdown
  ```

14.7. Pruebas de Conectividad

Se realizaron pruebas de ping entre dispositivos dentro de la misma VLAN y entre diferentes VLANs para evaluar la segmentación y la capacidad de enrutamiento entre las VLANs. Los resultados esperados fueron los siguientes:

- **Pruebas dentro de la misma VLAN:** Los dispositivos dentro de la misma VLAN se comunican sin problemas.
- **Pruebas entre VLANs diferentes:** Los dispositivos pertenecientes a VLANs diferentes no se comunican para segmentar la comunicación.

14.8. Resultados de las Pruebas de Tráfico

Para verificar el correcto funcionamiento de la segmentación y el enrutamiento entre VLANs, se observaron los siguientes resultados:

- **Dentro de la misma VLAN:** Pings exitosos con latencia baja y sin pérdida de paquetes entre los dispositivos de la misma VLAN.
- **Entre VLANs diferentes:** Pings exitosos entre dispositivos de diferentes VLANs, indicando que el enrutamiento entre VLANs fue configurado correctamente.

14.9. Conclusiones

Para realizar una conexión apropiada con enrutamiento de VLANs para el caso de esta red que no tiene router es necesario utilizar al menos un switch de capa 3, aunque en la simulación se utilizaron 3 switches del mismo modelo para facilitar la configuración de los mismos.

Al configurar los switches 1 y 2 se tienen que establecer las VLANs que se van a conectar a cada interfaz (canal de comunicación en un dispositivo de red) FastEthernet, para que se puedan comunicar o segmentar de la manera deseada los PC de la red.

La simulación demostró cómo el uso de VLANs puede mejorar la seguridad y la eficiencia de una red al segmentar el tráfico entre diferentes grupos de usuarios. Además, se comprobó la necesidad de contar con un switch de capa 3 para habilitar el enrutamiento entre VLANs sin la necesidad de un router dedicado.

Es importante verificar que las ip no esten duplicadas, porque podría causar varios problemas para la simulación, como paso en la práctica pero luego se volvió a configurar las ip de todos los dispositivos y se arreglo el duplicado.