UNIVERSIDAD TECNOLÓGICA DEL PERU

REDES Y COMUNICACIÓN DE DATOS I

Diseño e implementación de un Sistema de Streaming Seguro en Redes Virtuales usando Cisco Packet Tracer

INTEGRANTES

1.HILARIO CUCHO, JUAN PABLO

2. MEDINA NIÑO, FABRIZIO ADRIAN

3. OCSA CACERES, JUAN DIEGO

4. TAFUR PANDURO, JUAN MIGUEL ENRIQUE

5. YOLA SANCHEZ, JESHUA JOGAN

6. VELARDE OCHOA OBED VICTOR JESUS

DOCENTE

EDWIN PALOMINO IRIARTE

INDICE DE CONTENIDO

1. Introducción

El streaming representa el 82% del tráfico global de Internet (Cisco VNI, 2023), pero su transmisión insegura expone datos sensibles a sniffing, DDoS y robo de contenido. La convergencia de streaming de video y redes virtualizadas representa un desafío critico en redes modernas, donde la seguridad, baja latencia y aislamiento de tráfico son prioritarios. Este crecimiento exige redes capaces de manejar grandes volúmenes de datos con calidad y seguridad. Por ello, Cisco Packet Trace emerge como una herramienta accesible para simular estos entornos, validando configuraciones antes de su implementación física.

2. Objetivos

2.1. Objetivo General

Diseñar e implementar un modelo de red virtualizada en Cisco Packet Tracer que soporte streaming de video seguro, incorporando mecanismos de seguridad de red, con el fin de analizar su funcionamiento, rendimiento y vulnerabilidades en un entorno educativo.

2.2. Objetivos Específicos

- Diseñar y simular una red virtual segura en Cisco Packet Tracer que permite la transmisión eficiente de contenido multimedia.
- Configurar e implementar un sistema de streaming dentro de la red simulada, integrando servicios y protocolos adecuados para su funcionamiento.
- Aplicar y evaluar mecanismos de seguridad de red, como VLANs, ACLs y autenticación, para proteger la transmisión de datos y analizar posibles vulnerabilidades.

3. Problemática

3.1. Problemas Identificados

Las redes tradicionales basadas solo en VLANs y ACLs representan:

Congestión. Trafico de video compite con datos críticos.

Vulnerabilidades. ACLs no cifran datos.

Escalabilidad. Limitación de 4090 VLANs vs miles de dispositivos IoT.

3.2. Solución Propuesta

Se desarrollará una red de área local (LAN) virtual segmentadas en múltiples VLANs, diseñada para simular una transmisión segura de contenido vía streaming. La red se implementará y verificará en Cisco Packet Tracer, incluyendo funcionalidades reales como segmentación por VLAN, control de acceso mediando ACLs, enrutamiento interno, servicios de red (HTTP, SSH) y medidas de seguridad básicas.

4. Marco Teórico

VLAN. Mecanismo de segmentación lógica en capa 2 (OSI) que divide una red física en múltiples dominios de broadcast independientes, utilizando etiquetas IEE 802.1Q. Permite aislar dispositivos como si estuvieran en redes físicas separadas, mejorando la seguridad, eficiencia y gestión de trafico

QoS. Conjunto de técnicas para priorizar y gestionar el tráfico en una red, asegurando que aplicaciones sensibles (como video, voz o streaming) reciban ancho de banda, baja latencia y mínima pérdida de paquetes, incluso en condiciones de congestión.

SSH. Protocolo de capa 7 (aplicación) que permite acceso remoto seguro a dispositivos de red mediante un canal cifrado (AES-256). Reemplaza a Telnet al garantizar: Confidencialidad, Autenticación e Integridad.

HTTP. Protocolo de capa 7 (aplicación) para transferir contenido web (texto, imágenes, video) entre clientes y servidores. Opera bajo un modelo cliente-servidor mediante métodos como GET o POST. Limitación clave: No incluye cifrado nativo (requiere HTTPS/SSL para seguridad).

5. Diseño de la Red

5.1. Elementos de la red

El siguiente grafico muestra la cantidad de dispositivos y componentes a utilizar.

Dispositivo/Componente	Cantidad	Descripción/Función Principal
Router	1	Router principal con enrutamiento inter-VLAN (Router-on-a-Stick) y ACLs.
Switches	3	Switch(es) administrables para configurar VLANs.
PCs Clientes	15	Estaciones de trabajo en diferentes VLANs para simular usuarios.
Servidor HTTP/Streaming	1	Servidor que aloja el contenido multimedia simulado.
Servidor DHCP (opcional)	1	Para asignación dinámica de IP en la VLAN de invitados.
Cableado	-	Conexiones físicas simuladas entre dispositivos.
VLANs	3	Administración (VLAN 10), Usuarios Autorizados (VLAN 20), Invitados (VLAN 30).
ACLs	-	Para controlar acceso entre VLANs y hacia el servidor.
SSH	-	Habilitado en el router, acceso solo desde VLAN 10.

5.2. Estructura de VLANs y Subredes

El siguiente grafico muestra cómo se segmentó las VLANs y configuraciones a tener.

VLAN	Nombre	Propósito	Subred / Rango IP	Acceso permitido
10	Administración	Gestión de red y acceso SSH al router	192.168.10.0/24	Acceso completo al router por SSH
20	Usuarios Autorizados	Acceso al servidor de streaming	192.168.20.0/24	Acceso permitido al servidor HTTP
30	Invitados	Acceso limitado, solo red local	192.168.30.0/24	Sin acceso al servidor ni gestión del router

6. Implementación y Resultados

6.1. Tabla de Direccionamiento

El proyecto utiliza un esquema de direccionamiento IP segmentado por VLANs para la red, incluyendo VLANs para Administración, Usuarios Autorizados e Invitados.

- **Red de Administración (VLAN 10)**:
  - **Propósito**: Gestión de red y acceso SSH al router.
  - **Subred/Rango IP**: 192.168.10.0/24
  - **Acceso permitido**: Completo al router por SSH.
  - **Dispositivos**: PCAL, PCA2, PCA3, PCA4, PCA5 con IPs desde 192.168.10.1 hasta 192.168.10.5. El Gateway es 192.168.10.254.
  - **Switch de Administración**: IP 192.168.10.254.

Red de administración

Dispositivo	Dirección IP	Máscara Subred	Gateway	VLAN	Switch	Interfaz Dispositivo
PCA1	192.168.10.1	255.255.255.0	192.168.10.254	10	Switch Administración	Fa0/0
PCA2	192.168.10.2	255.255.255.0	192.168.10.254	10	Switch Administración	Fa0/1
PCA3	192.168.10.3	255.255.255.0	192.168.10.254	10	Switch Administración	Fa0/2
PCA4	192.168.10.4	255.255.255.0	192.168.10.254	10	Switch Administración	Fa0/3
PCA5	192.168.10.5	255.255.255.0	192.168.10.254	10	Switch Administración	Fa0/4
Router Subif G0/0.10	192.168.10.254	255.255.255.0	N/A	10	Switch Administración	G0/0.10

- **Red de Invitados (VLAN 20)**:
  - **Propósito**: Acceso limitado solo a red local.
  - **Subred/Rango IP**: 192.168.20.0/24
  - **Acceso permitido**: Sin acceso al servidor ni gestión del router.

- **Dispositivos**: PCII, PCI2, PCI3, PCI4, PCI5 con Ips desde 192.168.20.1 hasta 192.168.20.5. El Gateway es 192.168.20.254.
- **Switch de Invitados**: IP 192.168.20.254.

Red de invitados

Dispositivo	Dirección IP	Máscara Subred	Gateway	VLAN	Switch	Interfaz Dispositivo
PCI1	192.168.20.1	255.255.255.0	192.168.20.254	20	Switch Invitados	Fa0/0
PCI2	192.168.20.2	255.255.255.0	192.168.20.254	20	Switch Invitados	Fa0/1
PCI3	192.168.20.3	255.255.255.0	192.168.20.254	20	Switch Invitados	Fa0/2
PCI4	192.168.20.4	255.255.255.0	192.168.20.254	20	Switch Invitados	Fa0/3
PCI5	192.168.20.5	255.255.255.0	192.168.20.254	20	Switch Invitados	Fa0/4
Router Subif G0/0.20	192.168.20.254	255.255.255.0	N/A	20	Switch Invitados	G0/0.20

- **Red de Clientes (VLAN 30)**:
  - **Propósito**: Acceso al servidor de streaming.
  - **Subred/Rango IP**: 192.168.30.0/24
  - **Acceso permitido**: Al servidor HTTP.
  - **Dispositivos**: PCC1, PCC2, PCC3, PCC4, PCC5 con Ips desde 192.168.30.1 hasta 192.168.30.5, y el Servidor Streaming en 192.168.30.100. El Gateway es 192.168.30.254.
  - **Switch de Clientes**: IP 192.168.30.254.

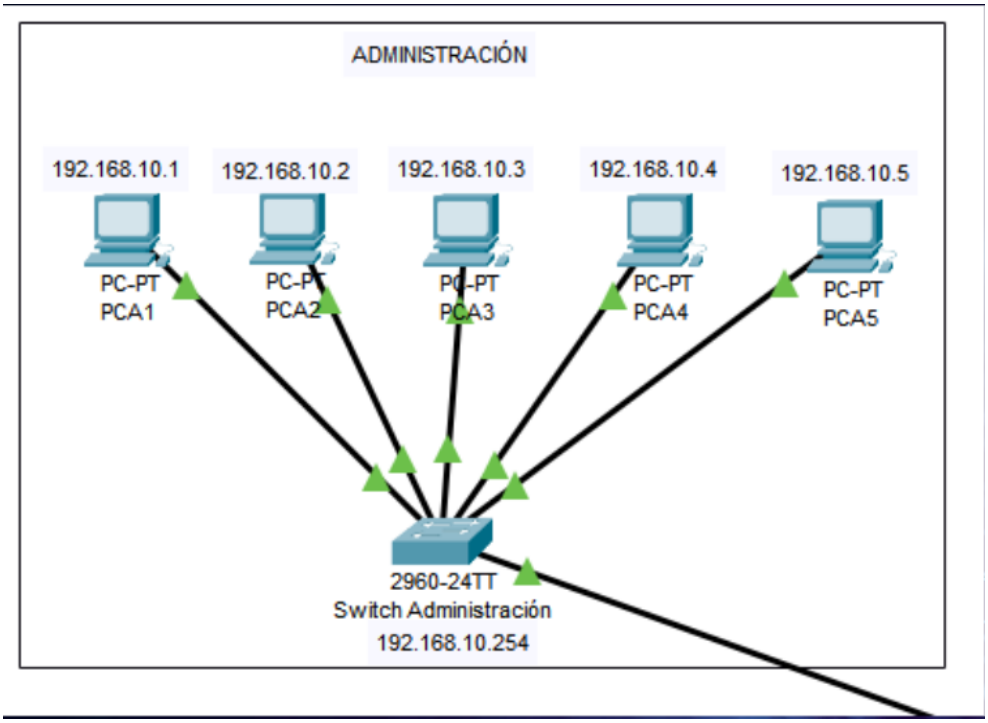
Red de Clientes

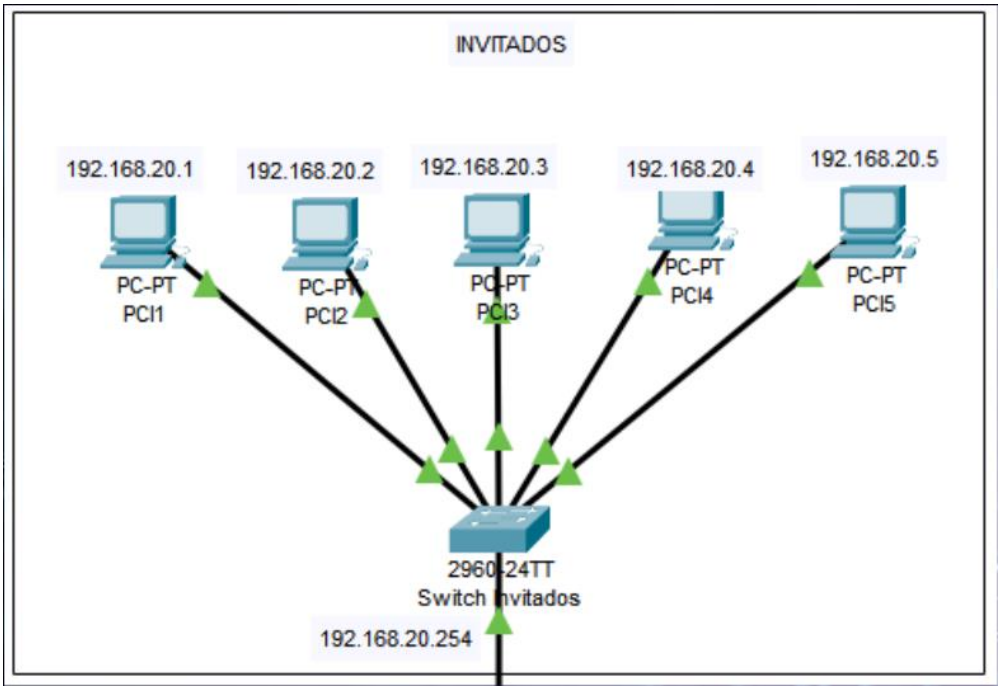
Dispositivo	Dirección IP	Máscara Subred	Gateway	VLAN	Switch	Interfaz Dispositivo
PCC1	192.168.30.1	255.255.255.0	192.168.30.254	30	Switch Clientes	Fa0/0
PCC2	192.168.30.2	255.255.255.0	192.168.30.254	30	Switch Clientes	Fa0/1
PCC3	192.168.30.3	255.255.255.0	192.168.30.254	30	Switch Clientes	Fa0/2
PCC4	192.168.30.4	255.255.255.0	192.168.30.254	30	Switch Clientes	Fa0/3
PCC5	192.168.30.5	255.255.255.0	192.168.30.254	30	Switch Clientes	Fa0/4
Servidor Streaming	192.168.30.100	255.255.255.0	192.168.30.254	30	Switch Clientes	Fa0/5
Router Subif G0/0.30	192.168.30.254	255.255.255.0	N/A	30	Switch Clientes	G0/0.30

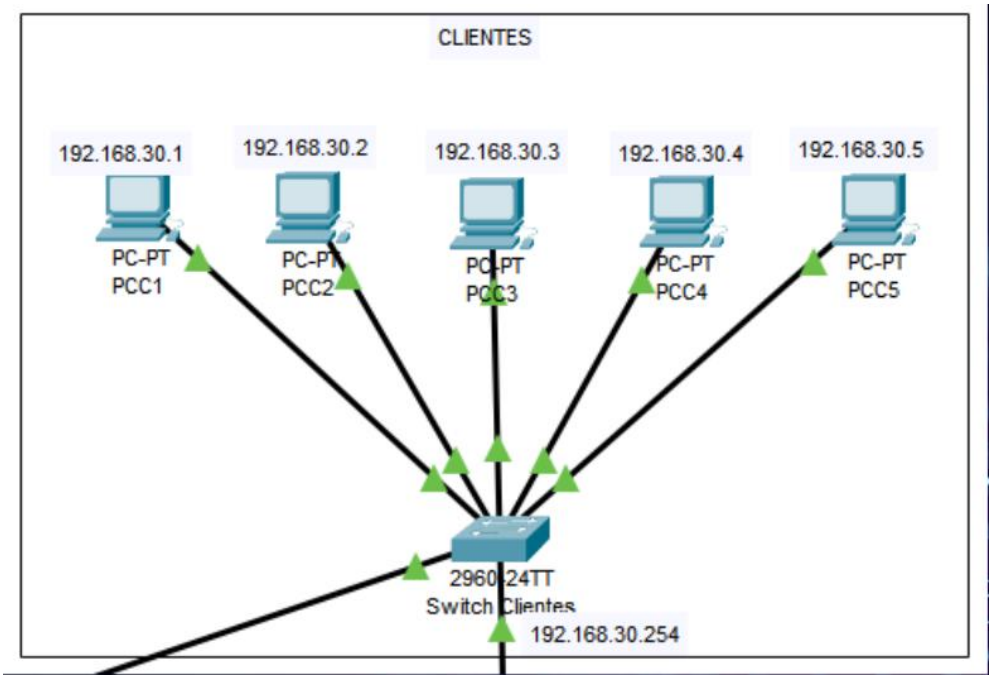
6.2. Topologia

La topología implementada es una red de área local (LAN) virtual segmentada en múltiples VLANs. Incluye un router principal con enrutamiento inter-VLAN (Router-on-a-Stick) y ACLs. Se utilizan switches administrables para configurar las VLANs, y quince PCs clientes distribuidas en diferentes VLANs para simular usuarios. Un servidor HTTP/Streaming aloja el contenido multimedia, y un servidor DHCP (opcional) es para la asignación dinámica de IP en la VLAN de invitados.

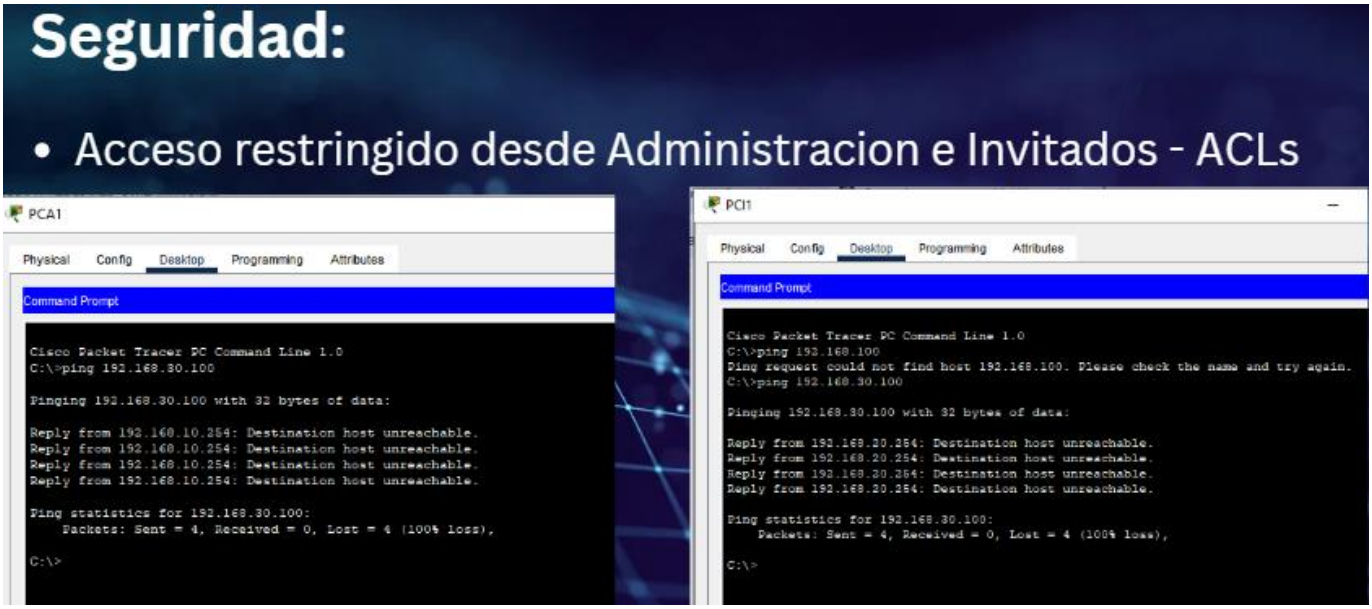
La topología principal muestra un Router Central conectado a un Switch Central. De este Switch Central, se desprenden conexiones a tres switches diferentes: Switch Administración, Switch Invitados y Switch Clientes. Cada uno de estos switches a su vez conecta a cinco PCs, representando las diferentes VLANs y sus respectivos usuarios.

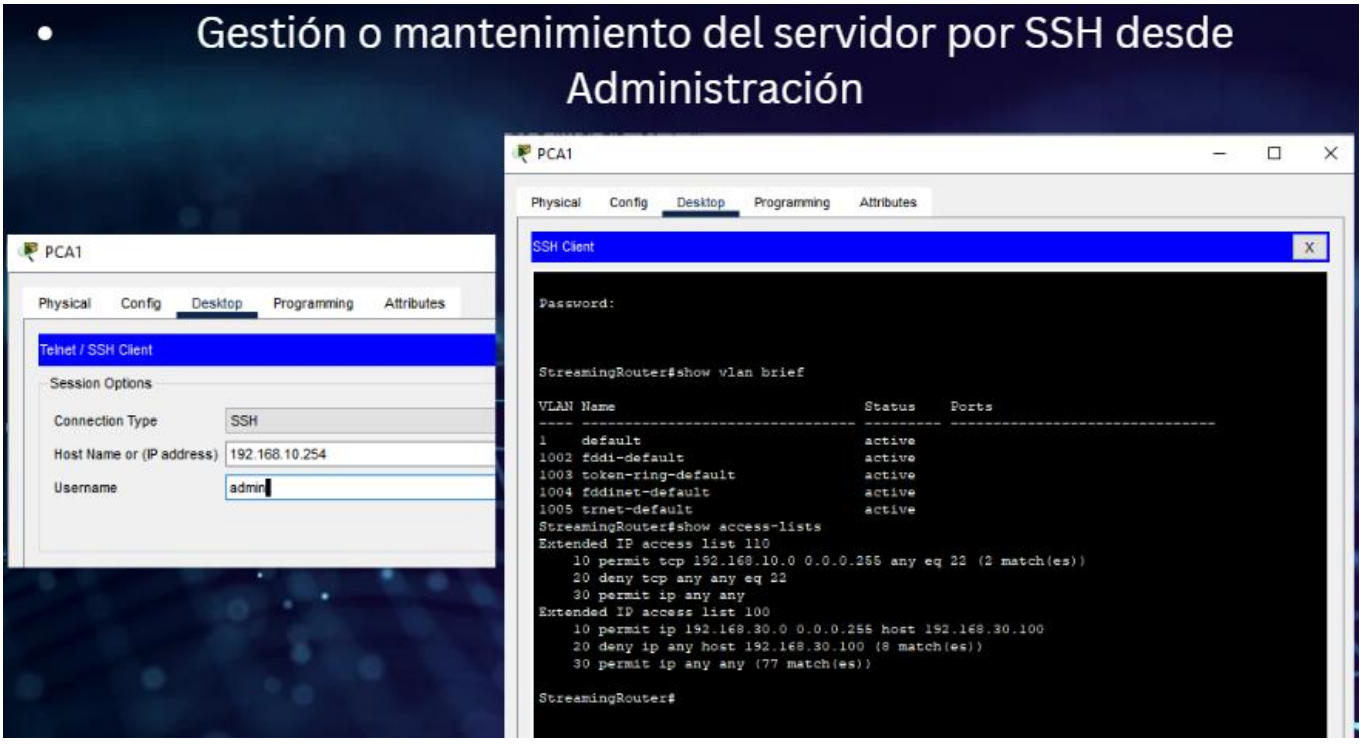

ADMINISTRACIÓN
192.168.10.1
192.168.10.2
192.168.10.3
192.168.10.4
192.168.10.5
PC-PT
PCA1
PC-PT
PCA2
PC-PT
PCA3
PC-PT
PCA4
PC-PT
PCA5
2960-24TT
Switch Administración
192.168.10.254


INVITADOS
192.168.20.1
192.168.20.2
192.168.20.3
192.168.20.4
192.168.20.5
PC-PT
PCI1
PC-PT
PCI2
PC-PT
PCI3
PC-PT
PCI4
PC-PT
PCI5
2960-24TT
Switch Invitados
192.168.20.254

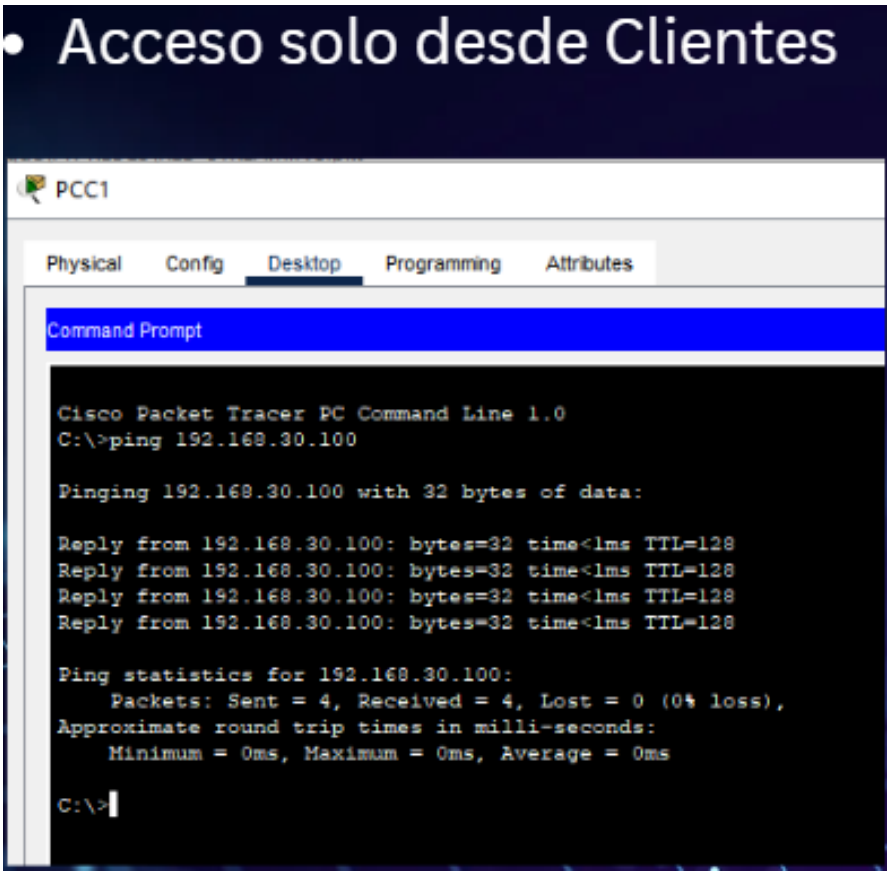

CLIENTES
192.168.30.1
192.168.30.2
192.168.30.3
192.168.30.4
192.168.30.5
PC-PT
PCC1
PC-PT
PCC2
PC-PT
PCC3
PC-PT
PCC4
PC-PT
PCC5
2960-24TT
Switch Clientes
192.168.30.254

6.3. Funcionamiento y Resultados



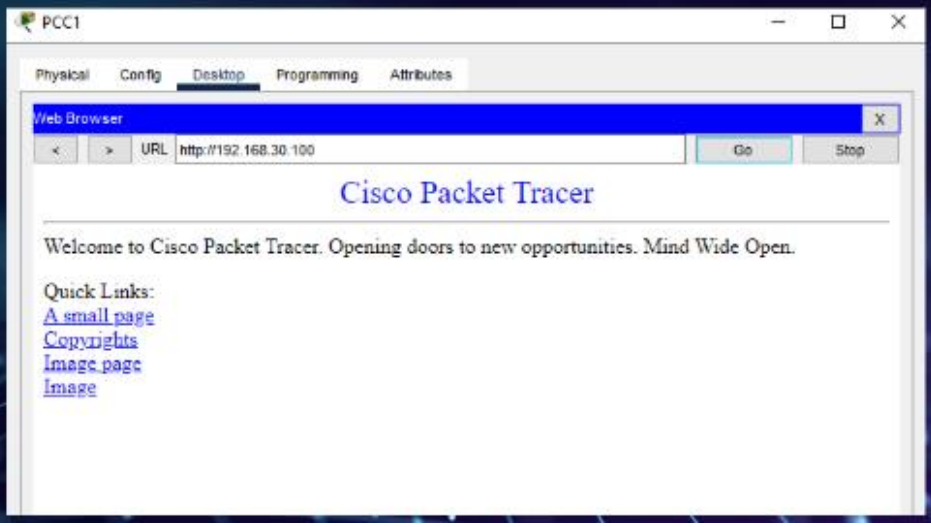


- Acceso solo desde Clientes

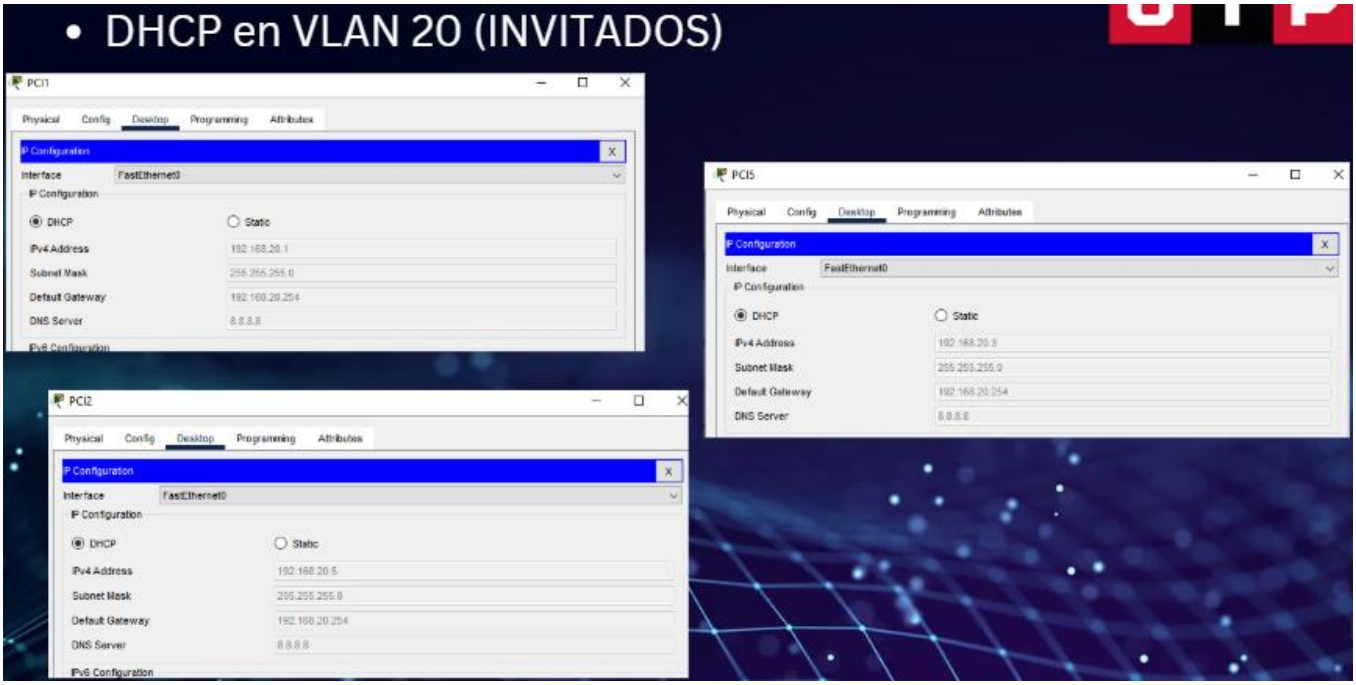


Servicios:

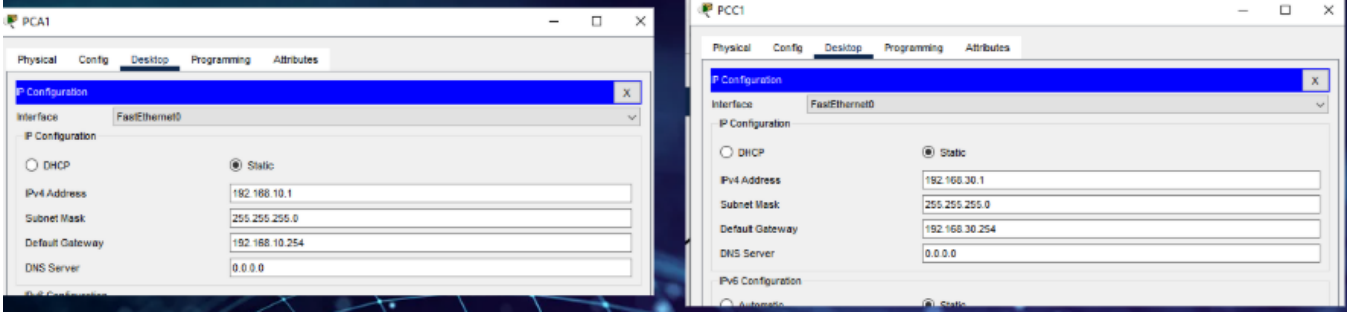
- HTTP para el servidor de streaming desde clientes



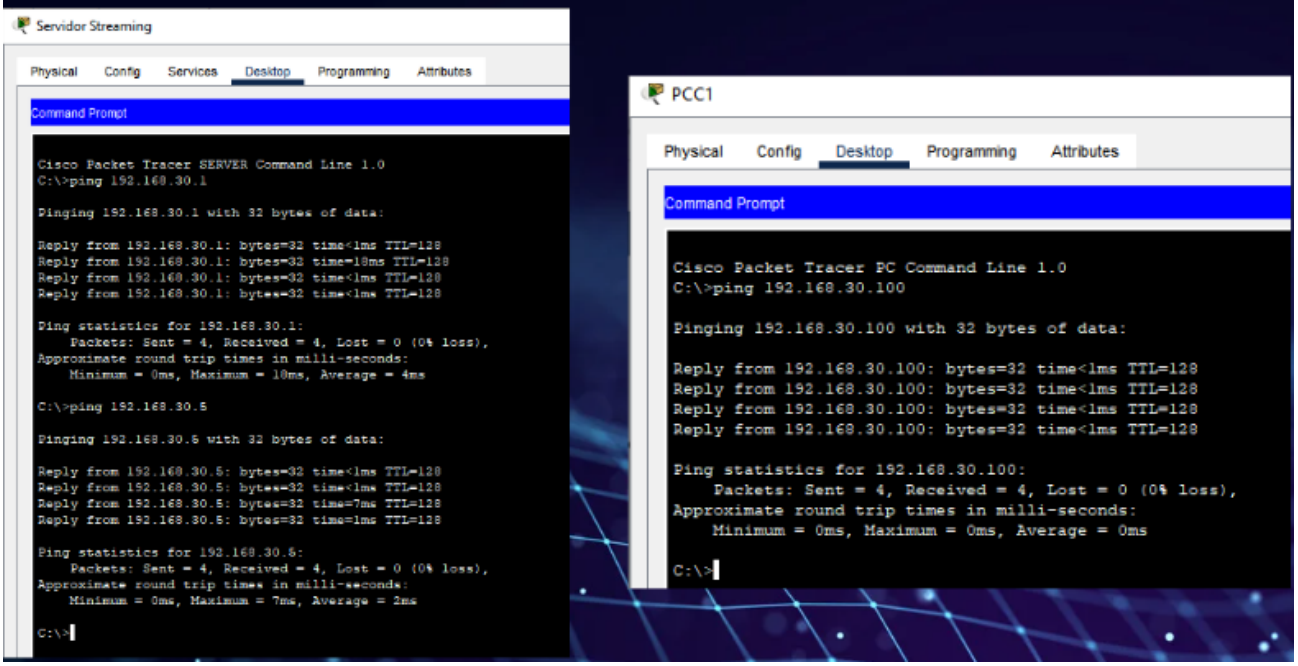
- DHCP en VLAN 20 (INVITADOS)



- IPs estaticas para Administración y Clientes



- Conexion bidireccional servidor - PC



Infraestructura

- Segementacion por VLAN 10, 20 , 30

```
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/4, Fa0/5, Fa0/6, Fa0/7
                                                Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24, Gig0/2
10   VLAN0010                         active
20   VLAN0020                         active
30   VLAN0030                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Switch#
```

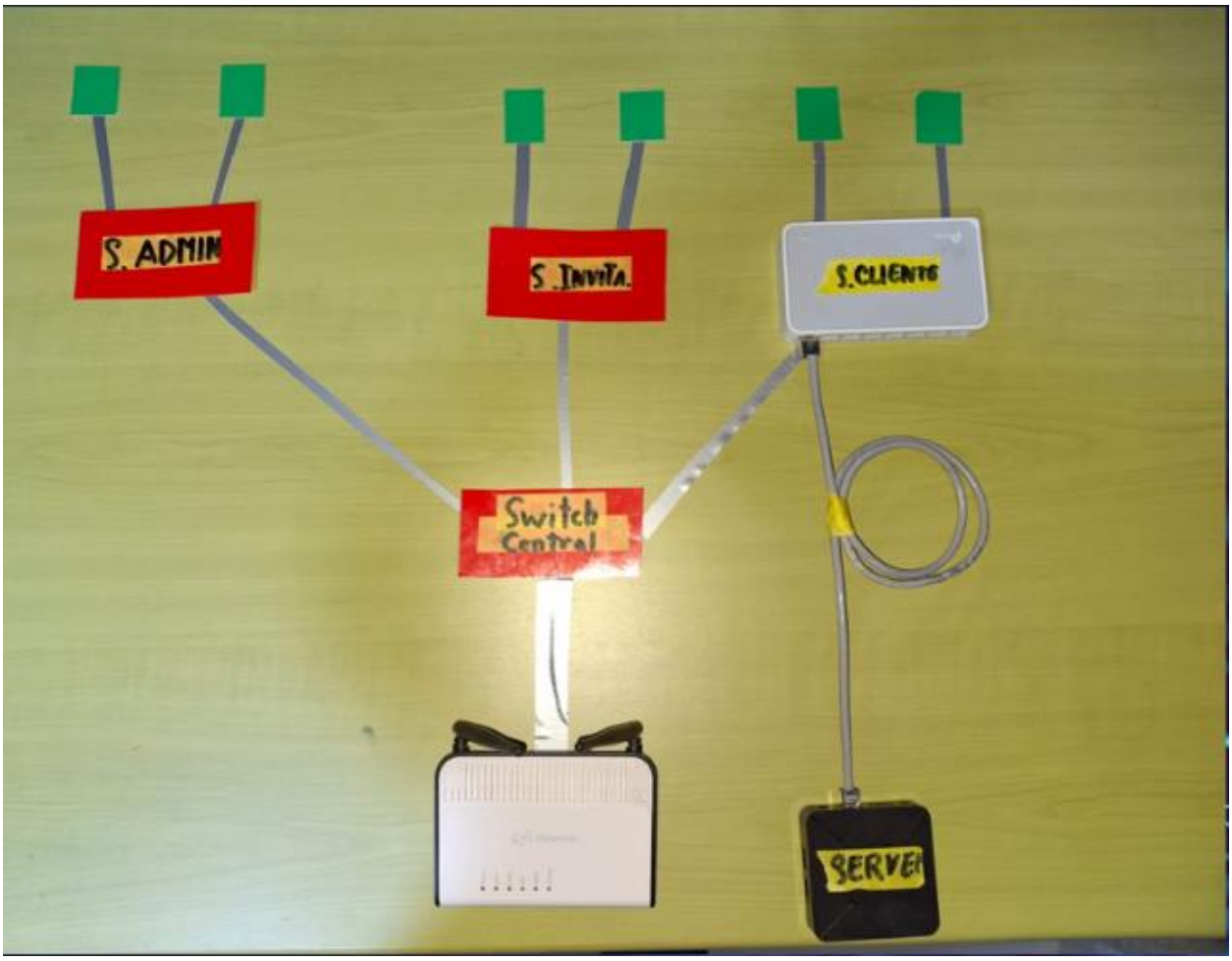
Copy Paste

7. Elaboracion de maqueta

7.1. Descripcion de la maqueta

Para complementar la simulación digital realizada en Cisco Packet Tracer, se elaboró una maqueta física que representa de manera visual y tangible la estructura lógica de la red implementada. Esta maqueta tiene como finalidad facilitar la comprensión del diseño de red y su segmentación por VLANs en un entorno educativo. La maqueta incluye los siguientes elementos:

- **Cinta gris**: Representa el cableado de red (UTP) que interconecta los distintos dispositivos.
- **Cartón rojo y verde**: Simula las etiquetas de identificación de cada segmento de la red o dispositivo, ayudando a diferenciar roles dentro del sistema.
- **Cinta amarilla**: Utilizada para sujetar el cableado y mantener ordenada la presentación.
- **Dispositivos simulados**:
    - **S. ADMIN**: Estación de trabajo del administrador, responsable de la gestión y supervisión de la red.
    - **S. INVITA**: Estación intermedia o cliente especial, que puede representar un usuario con permisos diferenciados.
    - **S. CLIENTE**: Representa el cliente final que consume el contenido en streaming.
    - **SERVER**: Simula el servidor de contenidos, desde donde se transmite el servicio de streaming.
    - **Switch Central**: Simula un switch gestionado con configuración VLAN para segmentar el tráfico entre dispositivos.
    - **Router (kit Marco Polo)**: Representa el dispositivo de interconexión con otras redes y servicios (como el acceso a internet o redes externas).



Se utilizó un Switch TP-Link real para reforzar el concepto de conmutación y segmentación de tráfico, además de una cajita negra como representación física del servidor. Todos los componentes están conectados de manera jerárquica, siguiendo una topología en estrella, donde el switch central es el núcleo de la comunicación.

8. Conclusiones y Recomendaciones

8.1. Conclusión

El desarrollo de este sistema de streaming seguro en redes virtuales mediante Cisco Packet Tracer demostró la viabilidad de crear entornos de transmisión multimedia eficientes y protegidos. La implementación de VLANs permitió una segmentación lógica de la red, aislando el tráfico crítico y mejorando tanto la seguridad como el rendimiento general. La integración de protocolos como SSH garantizó una administración remota segura, mientras que el uso de HTTP facilitó la simulación básica del servicio de streaming.

Los resultados mostraron que esta arquitectura puede manejar múltiples usuarios simultáneos manteniendo un rendimiento estable, con medidas de seguridad como listas de control de acceso (ACLs) que previnieron accesos no autorizados. La simulación en Packet Tracer confirmó que estas tecnologías, aunque básicas, son suficientes para entornos educativos o pequeñas implementaciones.

8.2. Recomendación

Para fortalecer el proyecto y llevarlo a un nivel más profesional, se sugiere implementar HTTPS en lugar de HTTP para garantizar la confidencialidad de los datos transmitidos. Sería valioso explorar el uso de firewalls de próxima generación para una protección más robusta contra amenazas cibernéticas. Considerar la implementación de autenticación multifactor añadiría una capa adicional de seguridad para el acceso al sistema. También se recomienda evaluar protocolos de streaming más eficientes como RTMP o HLS para mejorar la calidad de transmisión. La incorporación de herramientas de monitoreo en tiempo real permitiría detectar y resolver problemas de rendimiento de manera proactiva. Finalmente, sería beneficioso realizar pruebas de estrés con un mayor número de usuarios simultáneos para evaluar la escalabilidad real de la solución propuesta

9. Bibliografía

Implementar la calidad del servicio. (2025, February 28). Cisco. https://www.cisco.com/c/es_mx/support/docs/quality-of-service-qos/qos-packet-marking/13747-wantqos.html

Ejemplo de Configuración de Red Virtual Easy. (2022, March 14). Cisco. https://www.cisco.com/c/es_mx/support/docs/ip/ip-routing/117974-configure-evn-00.html

Cisco Annual Internet Report (2018–2023) white paper. (2022, January 23). Cisco. https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

Rodríguez, M. (2019). El streaming y nuevas formas de consumo en videojuegos. Recuperado de: http://hdl.handle.net/10554/46694