Guía laboratorio Interconexión de redes de computadoras

Paso a paso

La presente guía tiene como propósito enseñar el paso a paso llevado a cabo en el proyecto (Distri-Red), en el cual se estipula la metodología utilizada para diseñar, planificar y culminar el desarrollo del sistema de comunicación entre sedes. A continuación, se presenta de manera ordenada el proceso realizado.

Investigación

Se investigó un software capaz de simular el comportamiento de las conexiones tanto físicas como inalámbricas entre dispositivos, lo que llevó a seleccionar el simulador de redes **Cisco Packet Tracer**, un software proporcionado por la empresa CISCO, encargado de ofrecer herramientas educativas para el aprendizaje de redes y comunicaciones.

Durante esta fase se identificaron:

- Equipos disponibles (routers, switches, firewalls, servidores).
- Servicios necesarios (DNS, HTTP, FTP, DHCP, Email).
- Capacidades del entorno simulado (VLANs, subinterfaces, ACLs, servicios integrados).
- Limitaciones de Packet Tracer para entornos empresariales que involucraran ASA o autenticación real.

Esta investigación permitió establecer que el proyecto podía dividirse en **dos subsistemas.**

1. **Distri-Red (Plantel educativo)**:

   Red interna segmentada en VLANs con servicios corporativos y control de accesos.

2. **Empresa**:

   Simulación de infraestructura de red de una empresa con sucursal.

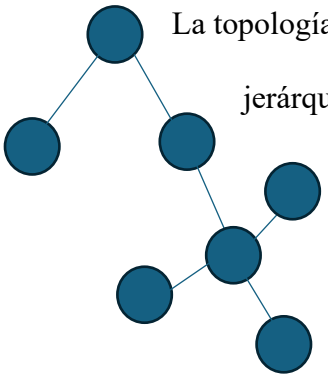
Planificación

Se definió una metodología de ejecución basada en cuatro etapas:

- Diseño conceptual de la red
- Diseño lógico mediante VLANs y subinterfaces
- Diseño físico/virtual dentro de Packet Tracer
- Aplicación de mecanismos de seguridad y pruebas

Diseño

Una vez investigado y planeado todo lo relacionado al proyecto, se procedió con el diseño de la topología general de la red



La topología más ideal para poder realizar ambos prototipos fue la del árbol jerárquico mixta, el cual combina la topología de árbol junto con la topología estrella.

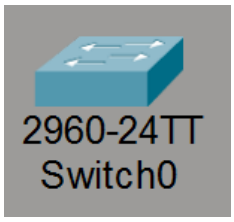
Una vez planteada la topología, se procede a la conexión y configuración de cada dispositivo

Conexión

Una vez finalizada la topología, se procedió a conectar cada equipo entre sí para poder configurarlos adecuadamente. En esta etapa, el elemento más importante fue la correcta selección del tipo de dispositivo y del medio físico apropiado para garantizar la comunicación entre todos los componentes de la red.

Durante este proceso se eligieron los siguientes equipos:

Se seleccionó el router Cisco 2911 debido a que es uno de los dispositivos más versátiles dentro de Packet Tracer para ambientes simulados. Y es bastante fácil de implementar acorde a la necesidad dentro de la red.



El Cisco 2960 es un switch de capa 2, diseñado para la conmutación dentro de una red local.

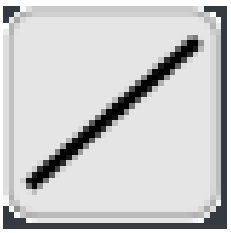
Su función principal es interconectar dispositivos finales dentro de un mismo segmento o VLAN, gestionando la entrega eficiente de tramas Ethernet.

El PC-PT simula un equipo final, equivalente a una computadora de escritorio dentro de una red local.

Es el dispositivo utilizado por los usuarios para realizar tareas cotidianas y probar conectividad.

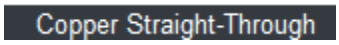
El Server-PT es un servidor multifuncional que permite simular diversos servicios dentro de una red.

Su propósito es actuar como un recurso centralizado al que acceden múltiples usuarios.

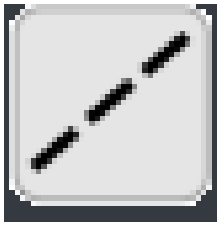


El cable directo es un tipo de cable Ethernet utilizado para conectar dispositivos diferentes entre sí.

Su configuración interna conecta pines de transmisión de un extremo

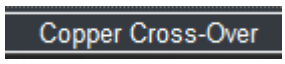


con pines de recepción del otro.



El cable cruzado es un cable Ethernet donde los pares de transmisión y recepción están invertidos.

Su función es permitir la conexión entre dispositivos del mismo tipo.



Prototipo de empresa de tecnologia

Configuración

En el primer prototipo se configuró de manera manual cada equipo, los servicios alojados en cada servidor, el switch que administra la red de la sede principal (HQ) y cada equipo de esta misma red, luego la configuracion del router, la configuracion del switch y servidor de la otra sucursal.

Switch de la sede principal: Se configuró para organizar la red por VLANs y asignar correctamente cada dispositivo según su función.
Primero, se crearon dos VLANs:

- **VLAN 10 (HQ)**: destinada a los equipos de los usuarios de la oficina principal.
- **VLAN 30 (SERVIDORES)**: destinada exclusivamente a los servidores centrales ubicados en esta sede.

Después se asignaron los puertos del switch a las VLAN correspondientes:
Los puertos donde estaban conectados los computadores de HQ se pusieron en VLAN 10, mientras que los puertos donde se ubicaban los servidores (DNS, DHCP, HTTP, FTP y correo) se asignaron a la VLAN 30.

Por último, el puerto que conecta el switch con el router se configuró como un enlace troncal (trunk) que transporta ambas VLANs hacia el router para permitir el enrutamiento entre ellas.

Switch sucursal:

En el switch de la sucursal se creó la **VLAN 20 (SUCURSAL)**, que reúne tanto a los equipos de usuario como al servidor de soporte local.

Los puertos donde se conectaron los PCs de la sucursal y el servidor de soporte se asignaron a esta VLAN.

Al igual que en el switch principal, el puerto que conecta al router se configuró como trunk para transportar la VLAN 20 hacia el router, permitiendo el enrutamiento con las demás VLANs.

Router:

El router actúa como el dispositivo central que interconecta las tres VLANs mediante subinterfaces.

Se configuraron dos interfaces físicas: una conectada al switch de HQ y otra al switch de la sucursal.

En la interfaz conectada a HQ se crearon dos subinterfaces:

- Una para VLAN 10, con la dirección IP que funcionará como puerta de enlace (gateway) de los usuarios de HQ.
- Otra para VLAN 30, con la puerta de enlace para los servidores.

En la interfaz conectada a la sucursal se creó la subinterfaz correspondiente a VLAN 20, asignándole su propia puerta de enlace.

Además, en las subinterfaces de las VLAN 10 y 20 se activó la función de DHCP Relay, indicando al router que debe redirigir cualquier solicitud DHCP hacia el servidor DHCP

ubicado en la VLAN 30.

Esto permite que tanto HQ como la sucursal obtengan direcciones IP automáticamente desde un servidor central.

Servidores:

En el prototipo de red se implementó un conjunto de servidores centrales ubicados en la VLAN 30, correspondiente a la sede principal (HQ), junto con un servidor adicional en la VLAN 20 de la sucursal destinado a garantizar continuidad operativa. Cada servidor cumple un rol específico dentro de la infraestructura, y todos fueron configurados con direcciones IP estáticas, dentro del segmento asignado a su VLAN, para asegurar estabilidad y fácil administración.

El servidor DHCP, ubicado en la VLAN 30, se configuró para gestionar la asignación automática de direcciones IP a los equipos de la sede principal (VLAN 10) y de la sucursal (VLAN 20). Se crearon dos pools independientes, cada uno con su puerta de enlace correspondiente, la misma dirección DNS de referencia y un rango de aproximadamente 50 direcciones disponibles. De esta manera, cualquier equipo conectado a la red puede obtener su configuración de forma inmediata a través del enrutamiento DHCP Relay realizado por el router.

El servidor DNS, también dentro de la VLAN de servidores, se configuró con una dirección IP fija y con el servicio DNS activado. En él se registraron los nombres de los distintos servicios internos, como el servidor HTTP, el servidor FTP y el servidor de correo, permitiendo que los usuarios puedan acceder a estos mediante nombres amigables en lugar de direcciones numéricas. Su función principal es resolver nombres dentro de la red interna,

garantizando una navegación fluida y coherente entre los diferentes servicios ofrecidos por la empresa.

El servidor HTTP fue configurado con su IP estática y el servicio web activado. Este servidor permite alojar páginas internas o contenidos informativos que pueden ser consultados desde cualquier equipo de la red. Cumple el rol de servidor web corporativo accesible tanto para HQ como para la sucursal mediante el enrutamiento inter-VLAN proporcionado por el router.

El servidor FTP, también con IP fija dentro de la VLAN 30, fue configurado para habilitar la transferencia de archivos entre las dos sedes. Este servicio facilita el intercambio rápido y seguro de información interna, evitando el uso de medios externos o correos electrónicos para compartir documentos entre áreas operativas.

Por su parte, el servidor de correo electrónico se configuró con su IP estática, con el servicio Email activado y con los buzones correspondientes. Este servidor permite realizar comunicación interna mediante cuentas locales, proporcionando un medio práctico para pruebas, mensajería interna o prácticas de administración de servicios de correo.

Finalmente, en la sucursal se configuró un servidor de soporte local, el cual utiliza una dirección IP estática dentro de la VLAN 20. Este servidor complementa la infraestructura central, actuando como componente de tolerancia a fallos: en caso de que la sede principal presente una caída o interrupción de servicios, la sucursal puede continuar operando gracias a este servidor alterno. Su función puede incluir servicios básicos o aplicaciones internas necesarias para la operación local, garantizando que la sucursal no dependa por completo de los servidores del HQ.

Computadores:

Todos los computadores se configuraron para obtener sus parámetros de red mediante DHCP.

Se comprobó que cada PC recibiera correctamente:

- Su dirección IP según su VLAN
- Su máscara de subred
- Su puerta de enlace
- Su DNS

Se realizaron pruebas de conectividad mediante ping a los servidores y entre sedes para validar el funcionamiento.

Pruebas de verificacion y conexión

Se ejecutaron pruebas de conectividad en las tres VLANs:

- Ping desde HQ hacia los servidores.
- Ping desde la sucursal hacia HQ.
- Prueba de acceso a HTTP, FTP y correo desde ambas sedes.
- Verificación de que los PCs obtuvieran IP por DHCP automáticamente.
- Comprobación de que el servidor de soporte en la sucursal estuviera disponible cuando la sede principal no respondiera.

Con esto se confirmó que el prototipo de red funciona correctamente, permite la comunicación completa entre sedes y garantiza continuidad operativa gracias al servidor local de la sucursal.

Prototipo plantel educativo

Configuración

En el prototipo Distri-Red se configuró manualmente cada dispositivo, incluyendo los switches de acceso, el switch principal, el router central, el servidor institucional y cada equipo final. La topología se diseñó para representar el funcionamiento de la red interna de un plantel educativo compuesto por varios departamentos, cada uno con requisitos de comunicación específicos.

La red fue segmentada mediante VLANs, se configuraron subinterfaces en el router para el enrutamiento inter-VLAN y se aplicaron ACLs para controlar el flujo de tráfico, garantizando la seguridad y las políticas internas de comunicación entre áreas.

A continuación, se describe el proceso tal como fue ejecutado.

Switch de la sede principal

El switch principal fue configurado para organizar la infraestructura mediante **VLANs**, separando lógicamente a cada departamento y permitiendo una administración eficiente. Se crearon las siguientes VLAN:

- **VLAN 10 – Administrativo**
- **VLAN 20 – Docentes**
- **VLAN 30 – Estudiantes**
- **VLAN 40 – Sede Primaria**
- **VLAN 50 – Sala de Sistemas (Sede Principal)**

- **VLAN 60 – Sala de Sistemas (Sede Primaria)**

Los puertos del switch principal se asignaron al trunk o acceso según su función:

- Los puertos que conectan a los switches de cada área se configuraron como trunk, transportando todas las VLAN necesarias.
- Los puertos conectados a equipos finales específicos fueron configurados como acceso.

Con esto, el switch principal quedó como el punto de distribución desde el cual se administra toda la comunicación entre las áreas educativas.

Switches de cada área

Cada laboratorio o departamento cuenta con su propio switch, configurado de acuerdo con su VLAN correspondiente.

Switch Administrativo – VLAN 10

Agrupa:

- PCs administrativos
- Impresora de oficina
- Servidor institucional

Switch Docente – VLAN 20

Conecta los puestos de trabajo del personal docente e impresora del área.

Switch Estudiantes – VLAN 30

Contiene solo terminales de estudiantes; su comunicación es altamente restringida.

Switch Sala de Sistemas – VLAN 50

Conecta los equipos del laboratorio de sistemas.

Esta VLAN está completamente aislada del resto de la red.

Switch Sede Primaria – VLAN 40

Contiene los equipos de la sede externa PRIMARIA, conectados por enlace troncal al router.

Switch Sala de Sistemas Sede Primaria – VLAN 60

Laboratorio informático de la sede primaria.

Queda totalmente independiente y aislado, igual que la VLAN 50.

Router

El router es el encargado de permitir el enrutamiento entre VLANs y aplicar las políticas de seguridad institucional.

Subinterfaces creadas

En la interfaz conectada al switch principal se configuraron subinterfaces:

- **G0/0.10 – VLAN 10 Administrativo**
- **G0/0.20 – VLAN 20 Docentes**

- **G0/0.30 – VLAN 30 Estudiantes**
- **G0/0.50 – VLAN 50 Sala de sistemas**

En la interfaz secundaria, conectada a la sede primaria:

- **G0/1.40 – VLAN 40 Sede Primaria**
- **G0/1.60 – VLAN 60 Sala de sistemas sede primaria**

Cada subinterfaz posee su propia IP, que también funciona como gateway para los dispositivos de su VLAN.

Seguridad mediante ACL

A diferencia de redes simples, Distri-Red requiere políticas estrictas de comunicación debido a la necesidad de proteger información sensible del área administrativa y evitar accesos indebidos desde estudiantes o laboratorios.

Por ello, se aplicaron ACL específicas en cada subinterfaz:

Políticas definidas:

- **Administrativo ↔ Docentes:** permitido
- **Administrativo ↔ Sede Primaria:** permitido
- **Docentes ↔ Estudiantes:** permitido
- **Estudiantes → Administrativo:** bloqueado
- **Estudiantes → Sede Primaria:** bloqueado

- **Estudiantes → Servidor web / correo / FTP:** bloqueado
- **Sala de Sistemas (VLAN 50 y 60):**
    - solo comunicación interna
    - cero comunicación externa (total aislamiento)
- **Acceso HTTP al portal:**
    - solo administradores, docentes y sede primaria
    - estudiantes y laboratorios no pueden ingresar

Estas ACL garantizan que cada departamento solo intercambie tráfico con las áreas permitidas y que ningún usuario no autorizado acceda a información protegida.

Servidor institucional

El servidor, ubicado en **VLAN 10 (Administrativo)**, fue configurado con dirección IP estática y actúa como centro de servicios de la institución.

Los servicios configurados fueron:

- **DNS:** resolución de los dominios internos
    - portal.colegio.edu
    - www.colegio.edu
    - mail.colegio.edu
    - ftp.colegio.edu
- **HTTP / Web:** portal institucional

    - Pantalla de login
    - Panel académico interno

- **FTP:** intercambio de archivos entre Docentes y Administrativos.
- **Correo institucional (SMTP/POP3):**
    - secretaria@colegio.edu
    - docente@colegio.edu

Computadores

Cada computadora fue configurada con:

- Dirección IP correspondiente a su VLAN
- Máscara de subred
- Gateway asignado
- DNS institucional

Además se probaron funciones esenciales:

- Ping entre áreas permitidas
- Bloqueos correctamente aplicados
- Acceso al correo
- Transferencias FTP
- Acceso al portal web

- Restricciones para Estudiantes y Salas de Sistemas

Los laboratorios (VLAN 50 y 60) cuentan con DHCP aislado y operativo.

Pruebas de verificación y conexión

Se realizaron pruebas para garantizar funcionalidad y seguridad:

- **Ping interno:** desde cada VLAN hacia su gateway.
- **Ping entre áreas permitidas:**

  Administrativo ↔ Docentes ↔ Estudiantes ↔ Sede Primaria
- **Bloqueos:**

  Estudiantes → Administrativo (bloqueado)

  Estudiantes → Sede Primaria (bloqueado)

  Estudiantes → Portal web (bloqueado)
- **Acceso al portal web:**

  ✓ VLAN 10

  ✓ VLAN 20

  ✓ VLAN 40

  ✗ VLAN 30 (no permitido)

  ✗ VLAN 50 y 60 (no permitido)
- **Correo institucional:**

  secretaria → docente (funcional)

- **FTP:**

  secretaria → docente (transferencia exitosa)

Todas las pruebas demostraron que la red opera conforme a las políticas establecidas.