



Proyecto final



Blanca Aracely Aranda Machorro

Monterrey Nuevo León

26-febrero-2025

Indicé:

Contenido

Infraestructura de red de TecmiCorp	3
Alcance:	3
Análisis y diseño	4
Desarrollo:	4
Implementación	7
Pruebas y Resultados:	9
Amenazas comunes:	16
Posibles ataques:	16
Medidas de seguridad:	16
Propuestas para una red confiable:	17
Glosario de términos y condiciones:	18
Bibliografía	20
Autores	22
Conclusiones y/o agradecimientos	24

Infraestructura de red de TecmiCorp



El Proyecto tiene como objetivo diseñar e implementar una infraestructura de red segura y escalable para TecmiCorp, una empresa en expansión con una sede central y cinco

sucursales. Se busca garantizar la conectividad confiable entre todas las ubicaciones, optimizando el rendimiento de la red y la seguridad.

Análisis y diseño

Se identificaron los siguientes requisitos para la implementación de la red:

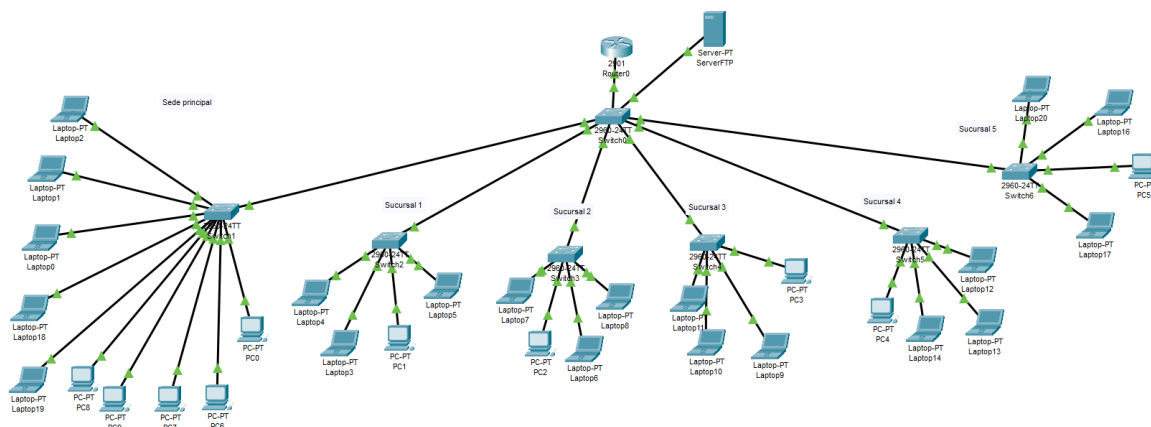
- Conectar 5 computadoras de escritorio y 5 laptops en la sede principal.
- Conectar 1 computadora de escritorio y 3 laptops en cada sucursal.
- Implementar una red con alta disponibilidad y escalabilidad.
- Implementar medidas de seguridad como firewalls y VPNs.

Para el diseño de la red se estructuró la conexión de la sede principal y las sucursales de la siguiente manera:

Para la sede principal se utilizó un switch y se conectó a este 5 laptops y 5 computadoras de escritorio, a cada dispositivo se le asignó una dirección IP.

Para las sucursales se utilizó 1 switch, a este se le conectaron 3 computadoras de escritorio y 1 laptop.

Cada una de las sucursales y la sede principal se conectó a un switch central para que estas estén conectadas entre sí y poder tener la comunicación entre sí.



Desarrollo:

El diseño de esta red fue desarrollado pensando en la escalabilidad, facilidad de administración y seguridad, garantizando una comunicación eficiente entre la sede

principal y las 5 sucursales. Este diseño nos permite una conexión estable y segura, optimizando el flujo de información y los procesos internos de la empresa.

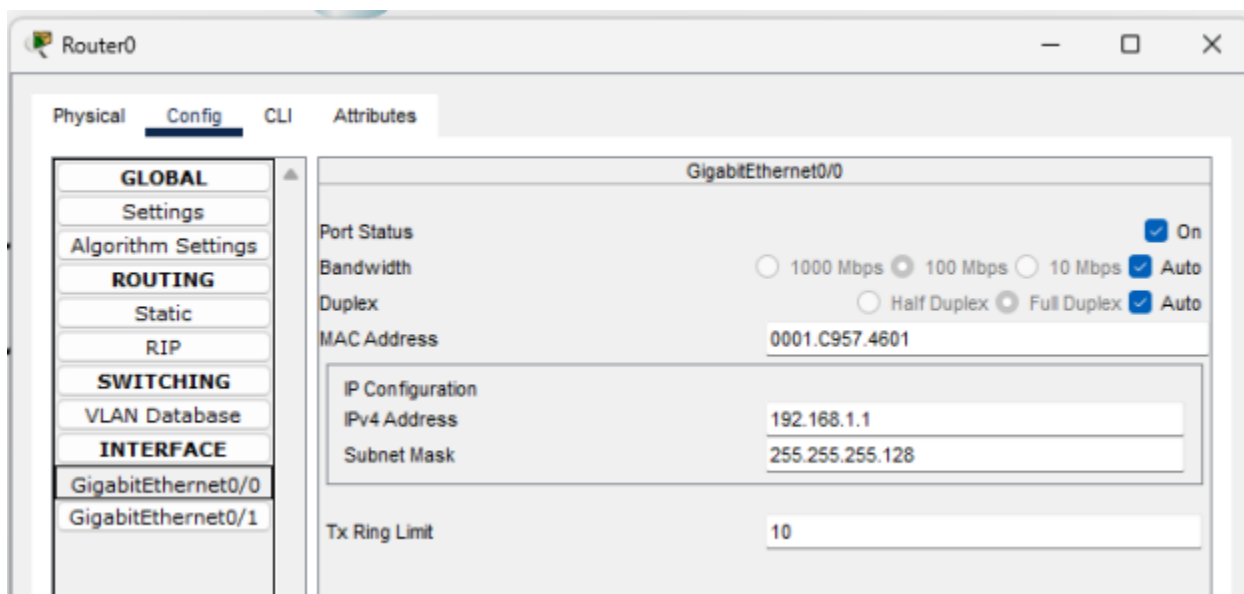
En la sede principal se utilizaron 5 computadoras de escritorio y 5 laptops para los trabajadores, como gerentes o administrativos que tengan el acceso a la información de la empresa, en las sucursales el diseño fue de una computadora de escritorio para el encargado de la sucursal y las laptops que se configuraron para que los clientes las utilicen.

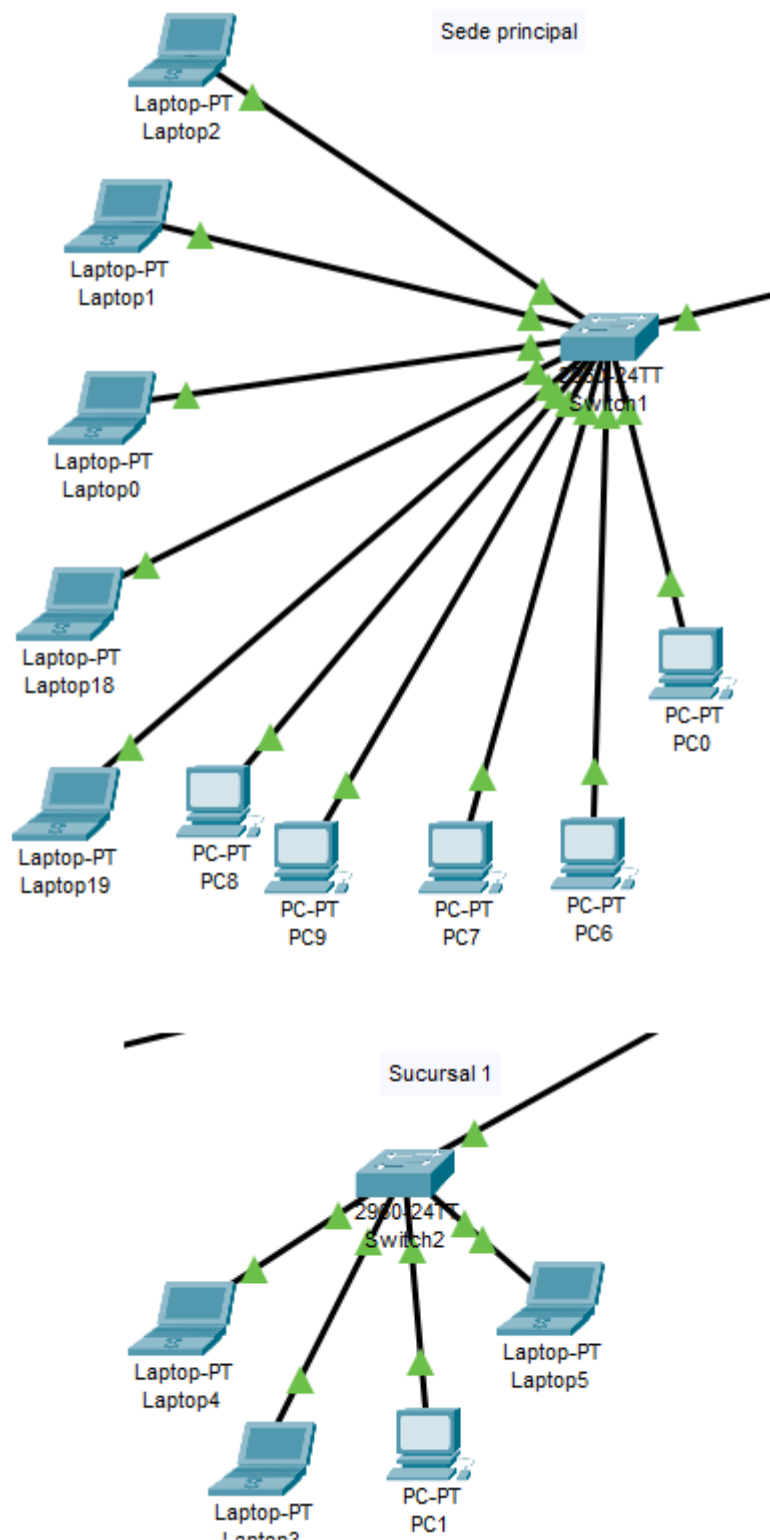
También se debe resaltar que el Router de la red principal tiene contraseña que solo la saben los que diseñaron la red para que no pasen problemas a futuro que puedan poner en riesgo la seguridad de la información de la empresa.

El desarrollo de la infraestructura de red incluyó las siguientes etapas:

1. Asignación de direcciones IP

- a. La sede principal utiliza el rango de IPs 192.168.1.2 - 192.168.1.11.
- b. Cada sucursal tiene su propio rango de IPs dentro de la subred 192.168.1.0/25.

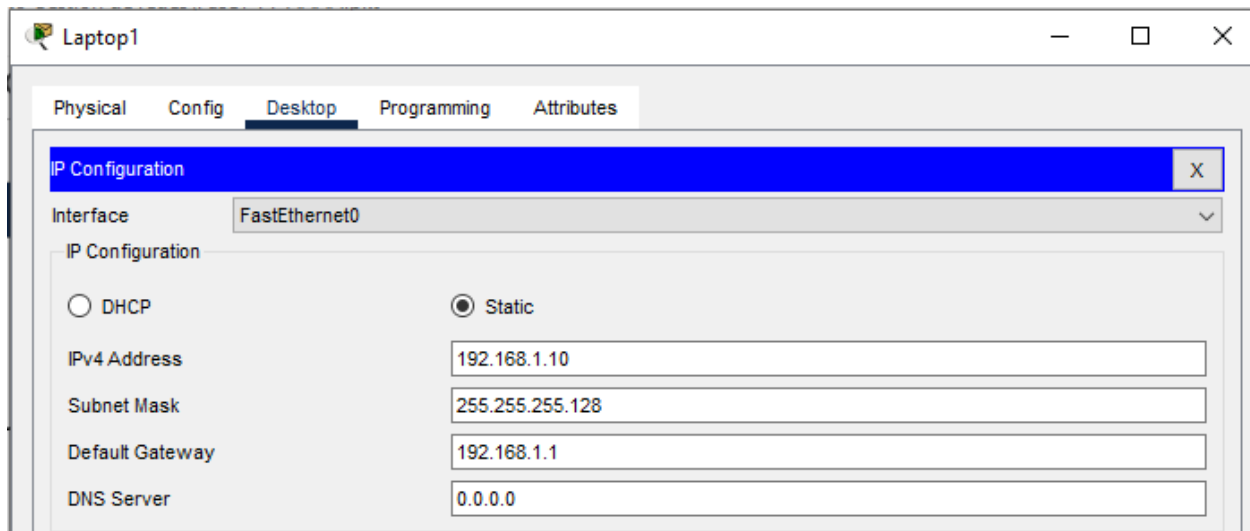




Cada sucursal cuenta con el mismo diseño, y cada equipo tiene asignada su IP ademas de su mascara.

2. Configuración de equipos

- a. Cada equipo tiene su IP asignada, por ejemplo, en la sede principal, cada laptop tiene su IP y su mask, además de su default Gateway:



3. Implementación de seguridad

- a. La red tiene un firewall para defender la red contra ataques DoS y bloquear intentos de acceso no autorizado a los routers con reglas de filtrado.

Implementación

Durante la implementación se configuraron y probaron todos los dispositivos de la red:

- Instalación y conexión de routers y switches.
- Configuración de puntos de acceso inalámbrico.
- Verificación de conectividad entre la sede principal y sucursales.

```
Laptop1
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 192.168.1.21

Pinging 192.168.1.21 with 32 bytes of data:

Reply from 192.168.1.21: bytes=32 time=1ms TTL=128
Reply from 192.168.1.21: bytes=32 time=5ms TTL=128
Reply from 192.168.1.21: bytes=32 time<1ms TTL=128
Reply from 192.168.1.21: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.21:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 5ms, Average = 1ms

C:\>ping 192.168.1.29

Pinging 192.168.1.29 with 32 bytes of data:

Reply from 192.168.1.29: bytes=32 time<1ms TTL=128
Reply from 192.168.1.29: bytes=32 time=4ms TTL=128
Reply from 192.168.1.29: bytes=32 time=6ms TTL=128
Reply from 192.168.1.29: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.29:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 6ms, Average = 2ms

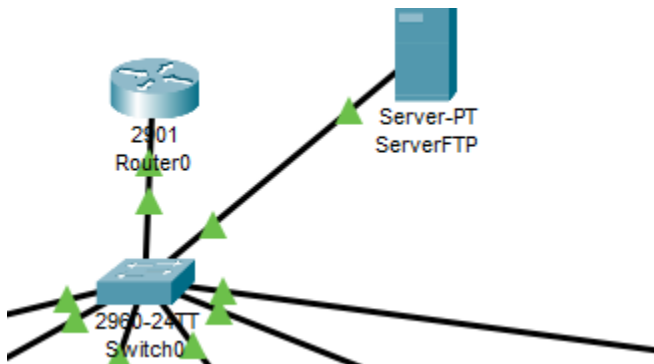
C:\>ping 192.168.1.6

Pinging 192.168.1.6 with 32 bytes of data:

Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128

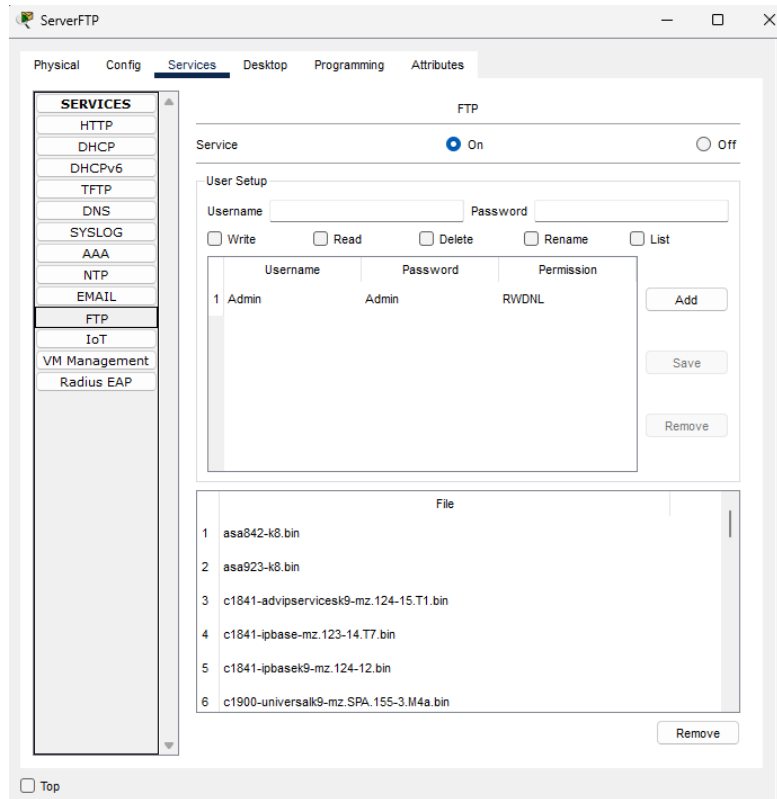
Ping statistics for 192.168.1.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

4. Implementación de servicio TFP



Se agrego un servidor a la red para poder usar el servicio FTP, al servidor se le agrego la IP 192.168.1.50 con la mask 255.255.255.128.

Se creo un servicio FTP con el nombre Admin y contraseña Admin que tiene todos los permisos que son: write, read, delete, rename y list.



Pruebas y Resultados:

Se realizaron diversas pruebas para validar la conectividad y seguridad de la red:

- **Pruebas de conectividad:** Se verificó la comunicación entre dispositivos con comandos de ping.

Laptop3

Physical Config Desktop Programming Attributes

Command Prompt

```
Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.1.20

Pinging 192.168.1.20 with 32 bytes of data:

Reply from 192.168.1.20: bytes=32 time<1ms TTL=128
Reply from 192.168.1.20: bytes=32 time<1ms TTL=128
Reply from 192.168.1.20: bytes=32 time<1ms TTL=128
Reply from 192.168.1.20: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.1.29

Pinging 192.168.1.29 with 32 bytes of data:

Reply from 192.168.1.29: bytes=32 time<1ms TTL=128
Reply from 192.168.1.29: bytes=32 time=6ms TTL=128
Reply from 192.168.1.29: bytes=32 time<1ms TTL=128
Reply from 192.168.1.29: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.29:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 6ms, Average = 1ms
```

Laptop10

Physical Config Desktop Programming Attributes

Command Prompt

```
C:\>ping 192.168.1.6

Pinging 192.168.1.6 with 32 bytes of data:

Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.1.27

Pinging 192.168.1.27 with 32 bytes of data:

Reply from 192.168.1.27: bytes=32 time<1ms TTL=128
Reply from 192.168.1.27: bytes=32 time<1ms TTL=128
Reply from 192.168.1.27: bytes=32 time<1ms TTL=128
Reply from 192.168.1.27: bytes=32 time<1ms TTL=128

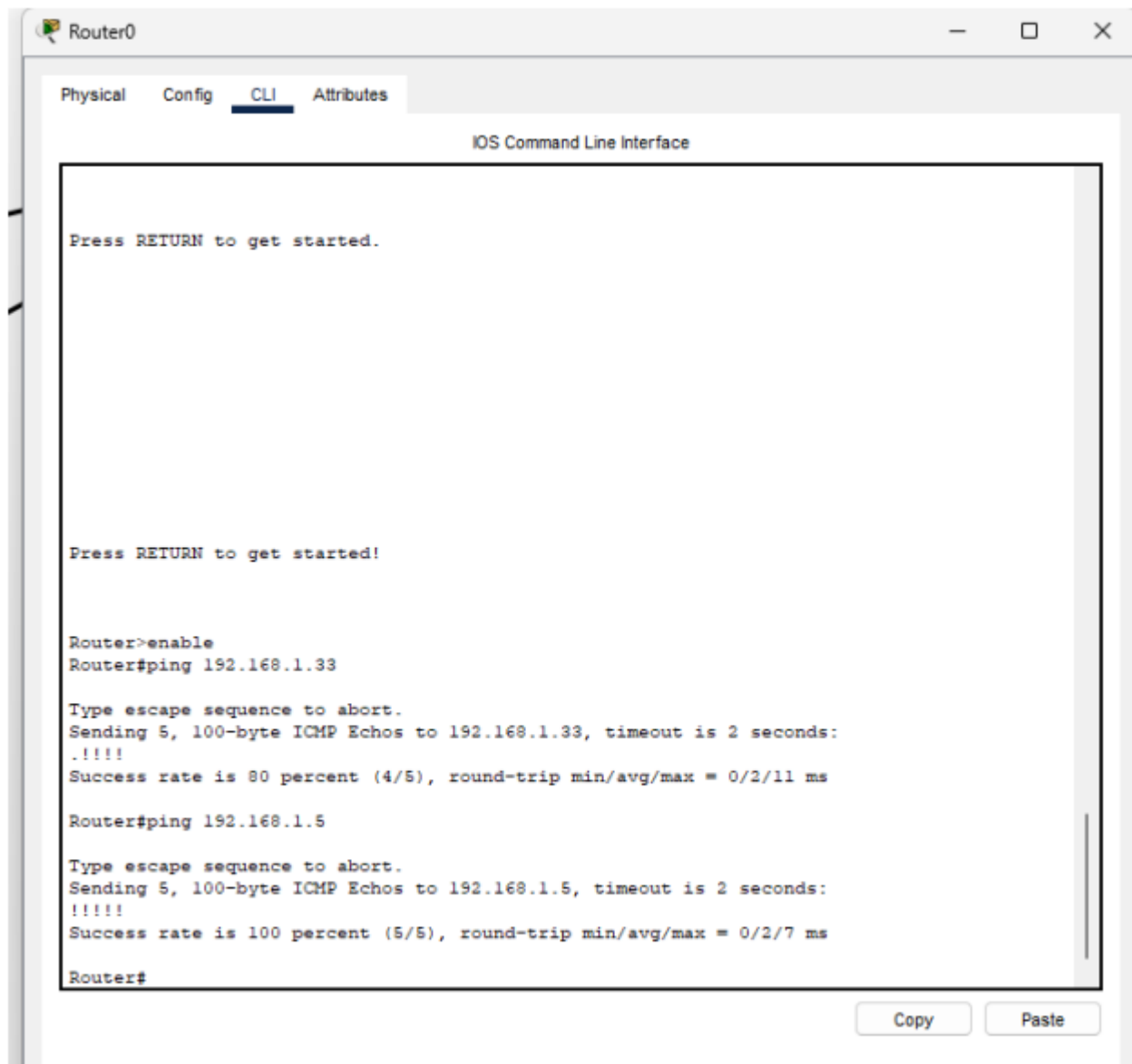
Ping statistics for 192.168.1.27:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.1.18

Pinging 192.168.1.18 with 32 bytes of data:

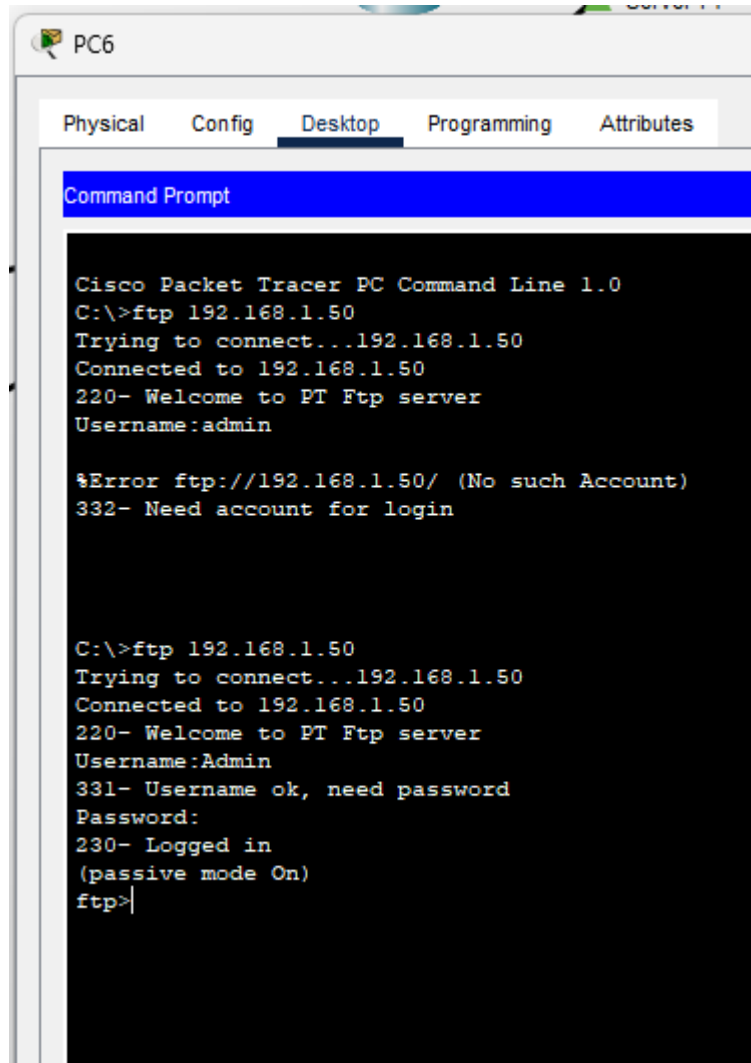
Reply from 192.168.1.18: bytes=32 time=5ms TTL=128
Reply from 192.168.1.18: bytes=32 time<1ms TTL=128
Reply from 192.168.1.18: bytes=32 time=2ms TTL=128
Reply from 192.168.1.18: bytes=32 time=4ms TTL=128

Ping statistics for 192.168.1.18:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```



- **Pruebas de segmentación:** Se validó el aislamiento de tráfico mediante VLANs.
- **Pruebas de seguridad:** Se simularon ataques de fuerza bruta y MITM para evaluar la efectividad de las protecciones implementadas.

- Pruebas de servicio FTP:

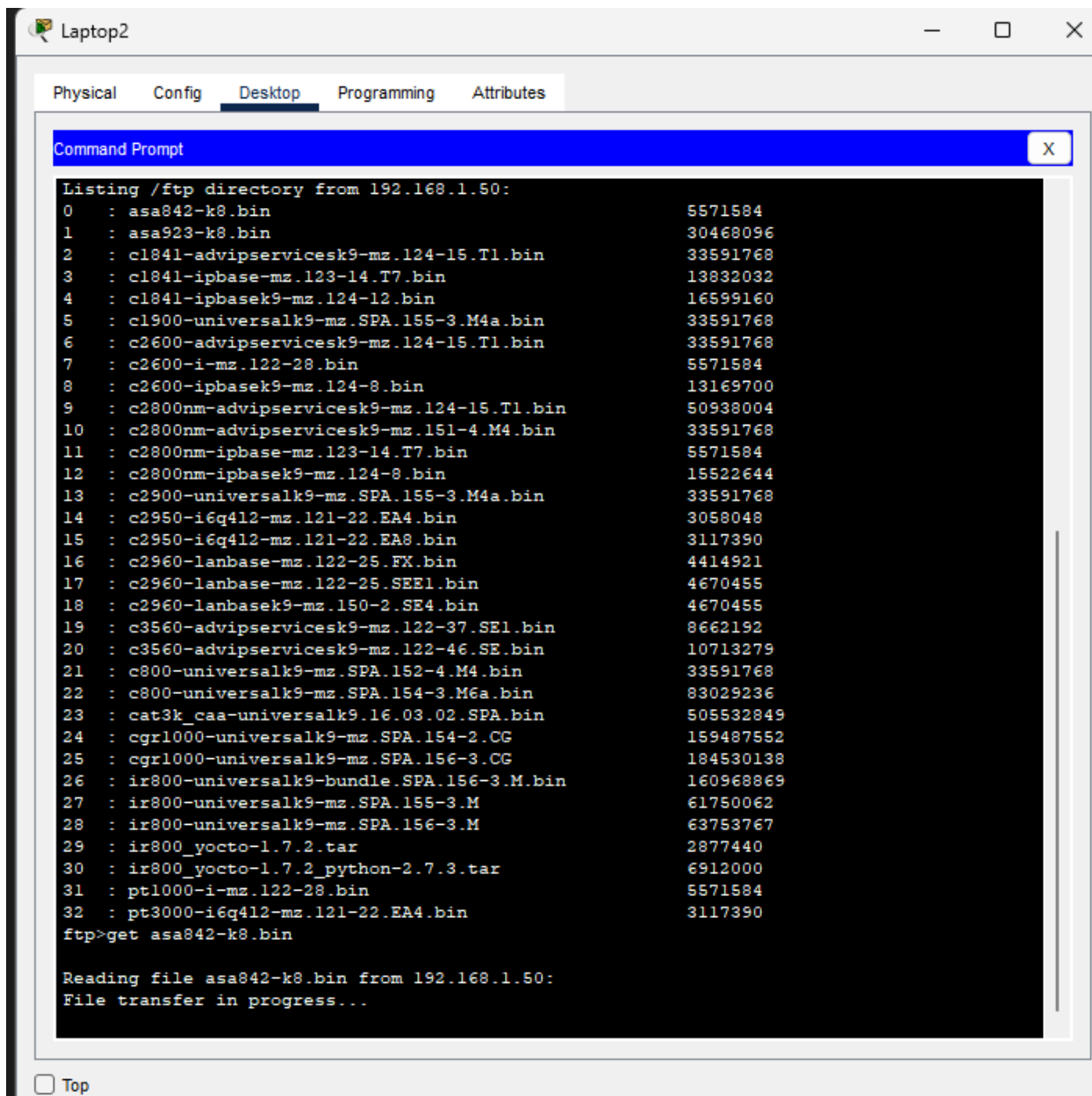


The screenshot shows a PC6 window in Cisco Packet Tracer with the 'Desktop' tab selected. A 'Command Prompt' window is open, displaying the following text:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 192.168.1.50
Trying to connect...192.168.1.50
Connected to 192.168.1.50
220- Welcome to PT Ftp server
Username:admin

%Error ftp://192.168.1.50/ (No such Account)
332- Need account for login

C:\>ftp 192.168.1.50
Trying to connect...192.168.1.50
Connected to 192.168.1.50
220- Welcome to PT Ftp server
Username:Admin
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```



Laptop2

Physical Config Desktop Programming Attributes

Command Prompt

```
3 : c1841-ipbase-mz.123-14.T7.bin 13832032
4 : c1841-ipbasek9-mz.124-12.bin 16599160
5 : c1900-universalk9-mz.SPA.155-3.M4a.bin 33591768
6 : c2600-advipervicesk9-mz.124-15.T1.bin 33591768
7 : c2600-i-mz.122-28.bin 5571584
8 : c2600-ipbasek9-mz.124-8.bin 13169700
9 : c2800nm-advipervicesk9-mz.124-15.T1.bin 50938004
10 : c2800nm-advipervicesk9-mz.151-4.M4.bin 33591768
11 : c2800nm-ipbase-mz.123-14.T7.bin 5571584
12 : c2800nm-ipbasek9-mz.124-8.bin 15522644
13 : c2900-universalk9-mz.SPA.155-3.M4a.bin 33591768
14 : c2950-i6q412-mz.121-22.EA4.bin 3058048
15 : c2950-i6q412-mz.121-22.EA8.bin 3117390
16 : c2960-lanbase-mz.122-25.FX.bin 4414921
17 : c2960-lanbase-mz.122-25.SEE1.bin 4670455
18 : c2960-lanbasek9-mz.150-2.SE4.bin 4670455
19 : c3560-advipervicesk9-mz.122-37.SE1.bin 8662192
20 : c3560-advipervicesk9-mz.122-46.SE.bin 10713279
21 : c800-universalk9-mz.SPA.152-4.M4.bin 33591768
22 : c800-universalk9-mz.SPA.154-3.M6a.bin 83029236
23 : cat3k_caa-universalk9.16.03.02.SPA.bin 505532849
24 : cgr1000-universalk9-mz.SPA.154-2.CG 159487552
25 : cgr1000-universalk9-mz.SPA.156-3.CG 184530138
26 : ir800-universalk9-bundle.SPA.156-3.M.bin 160968869
27 : ir800-universalk9-mz.SPA.155-3.M 61750062
28 : ir800-universalk9-mz.SPA.156-3.M 63753767
29 : ir800_yocto-1.7.2.tar 2877440
30 : ir800_yocto-1.7.2_python-2.7.3.tar 6912000
31 : pt1000-i-mz.122-28.bin 5571584
32 : pt3000-i6q412-mz.121-22.EA4.bin 3117390
ftp>get asa842-k8.bin

Reading file asa842-k8.bin from 192.168.1.50:
File transfer in progress...

[Transfer complete - 5571584 bytes]

5571584 bytes copied in 36.679 secs (34805 bytes/sec)
```

Amenazas comunes:

El acceso no autorizado, es una amenaza tanto interna como externa, los usuarios sin permisos pueden acceder a dispositivos críticos y hackers externos podrían explotar configuraciones débiles.

Ataques de denegación de servicio, es una amenaza externa. Al tener un solo router, un ataque DDoS podría saturar la red.

Intercepción de datos, es una amenaza interna y externa. Un atacante podría interceptar paquetes de red sin cifrado.

Infección por malware, es una amenaza interna y externa. Dispositivos infectados pueden propagar virus o ransomware.

Errores de configuración, es una amenaza interna. Configuraciones incorrectas en el router o switch pueden crear vulnerabilidades.

Posibles ataques:

Ataque MITM: un Atacante puede interceptar y modificar datos transmitidos debido a la falta de cifrado.

Spoofing de ARP: un atacante interno puede falsificar direcciones MAC y redirigir el tráfico.

Ataques por fuerza bruta en el router: si el router tiene credenciales débiles, un atacante externo podría tomar el control.

Medidas de seguridad:

Implementar autenticación fuerte en el router y switches

Usar contraseñas seguras y autenticación de multifactor (MFA). **Beneficio:** Reduce el riesgo de accesos no autorizados.

Configurar VLANs y segmentación de red

Separar el tráfico de la sede principal y sucursales con VLANs. **Beneficio:** Reduce el impacto de ataques internos.

Activar cifrado en las comunicaciones Usar VPNs para conexiones entre sucursales. **Beneficio:** Protege los datos de intercepción.

Filtrar tráfico con listas de control de acceso (ACLs)

Limitar qué dispositivos pueden comunicarse con el router. **Beneficio:** Bloquea accesos no autorizados.

Monitoreo y registro de eventos en la red

Implementar syslog y SNMP para detectar ataques en tiempo real. **Beneficio:** Permite respuesta rápida a incidentes.

Propuestas para una red confiable:

Para poder mejorar la confiabilidad de la red de TecmiCorp se debería de agregar un segundo router para permitir continuidad del servicio si el router principal falla.

Configurar protocolos de enrutamiento dinámico para automatizar la gestión del tráfico y mejora la escalabilidad.

Implementar un firewall perimetral que proteja contra amenazas externas y filtra tráfico malicioso.

Usar servicios de autenticación para controlar el acceso administrativo a los dispositivos de red

Glosario de términos y condiciones:



- **VPN (Virtual Private Network):** Red privada virtual utilizada para conexiones seguras.
- **VLAN (Virtual Local Area Network):** Segmentación de red para mejorar seguridad y rendimiento.
- **Firewall:** Sistema de seguridad que filtra el tráfico de red.
- **Router:** Dispositivo que gestiona el tráfico de datos entre redes.
- **Switch:** Dispositivo que conecta múltiples dispositivos en una red.
- **NAT (Network Address Translation):** Método de mapeo de direcciones IP para permitir que varios dispositivos compartan una única dirección IP pública.
- **SSID (Service Set Identifier):** Nombre que identifica una red WiFi.
- **Autenticación WPA3:** Protocolo de seguridad para redes inalámbricas que mejora la protección contra ataques de fuerza bruta.
- **Segmentación de red:** Técnica utilizada para dividir una red en subredes más pequeñas para mejorar la seguridad y el rendimiento.
- **Ping:** Comando utilizado para verificar la conectividad entre dispositivos en una red.
- **Dirección IP (Internet Protocol):** Identificador único asignado a un dispositivo en una red.
- **Default Gateway:** Dirección IP del router utilizada para la comunicación entre redes diferentes.

Bibliografía



Cisco Packet Tracer. (s/f). Netacad.com. Recuperado el 28 de febrero de 2025, de

<https://www.netacad.com/courses/packet-tracer>

Cisco Packet Tracer 8.2.2 : Download free labs and tutorials for CCNA v7 certification exam preparation. (s/f). Packet Tracer Network. Recuperado el 28 de febrero de 2025, de
<https://www.packettracernetwork.com>

(S/f-a). Learnpackettracer.com. Recuperado el 28 de febrero de 2025, de <https://www.learnpackettracer.com>

(S/f-b). Guru99.com. Recuperado el 28 de febrero de 2025, de <https://www.guru99.com/cisco-packet-tracer.html>

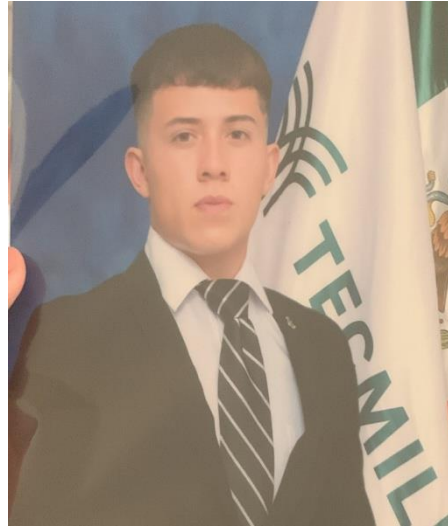
(S/f-c). Packettraceracademy.com. Recuperado el 28 de febrero de 2025, de <https://www.packettraceracademy.com>

Autores





Ángel Austrer Agüero Ávila



Patricio Didier Ramírez Martínez

Conclusiones y/o agradecimientos



El desarrollo e implementación de la infraestructura de red para TecmiCorp ha permitido establecer una conectividad segura y escalable entre la sede principal y sus cinco sucursales. La aplicación de tecnologías como VLANs, firewalls y VPNs ha mejorado la seguridad y el rendimiento de la red, asegurando una comunicación estable entre los distintos puntos de la empresa.

Se lograron los objetivos planteados, incluyendo la segmentación eficiente del tráfico, la optimización de los recursos de red y la integración de mecanismos de autenticación robustos. Las pruebas realizadas han validado el correcto funcionamiento de la infraestructura, asegurando su capacidad para soportar el crecimiento de la empresa.

Este proyecto demuestra la importancia de un diseño de red bien estructurado, permitiendo una administración eficiente y segura de los recursos tecnológicos.

Agradecemos a nuestra maestra por la explicación de esta materia.