



Diseño e Implementación de una Red Informática para una Pequeña Empresa

En el presente proyecto se ha diseñado e implementado una red informática simulada para una pequeña empresa con 75 empleados, utilizando la herramienta Cisco Packet Tracer. El objetivo principal ha sido construir una infraestructura de red eficiente, segura y escalable que permita la conexión de 50 estaciones de trabajo cableadas y 25 dispositivos vía WiFi, junto con un servidor centralizado.

Arantxa Quijada López

Rumen Orachev Orachev

Javier Canudo Távara

Stanislav Muntyan

Fig. 1. Plano de la empresa.

Hardware y Software de los Equipos y Servidores

Hardware

- Tipos de Equipo: Escritorios y portátiles (ej. Dell OptiPlex 7010, HP ProBook 450 G9)
- Especificaciones Comunes:
 - CPU: Intel i5-12400 / AMD Ryzen 5 5600U
 - RAM: 16 GB DDR4
 - Almacenamiento: SSD 512 GB NVMe
 - Pantalla (portátil): 15.6" FHD IPS
 - Gráficos: Integrados (Intel UHD / Radeon)
 - SO: Windows 11 Pro (activado)
 - Estado: Operativo / Mantenimiento / Con fallas

Red y Comunicaciones

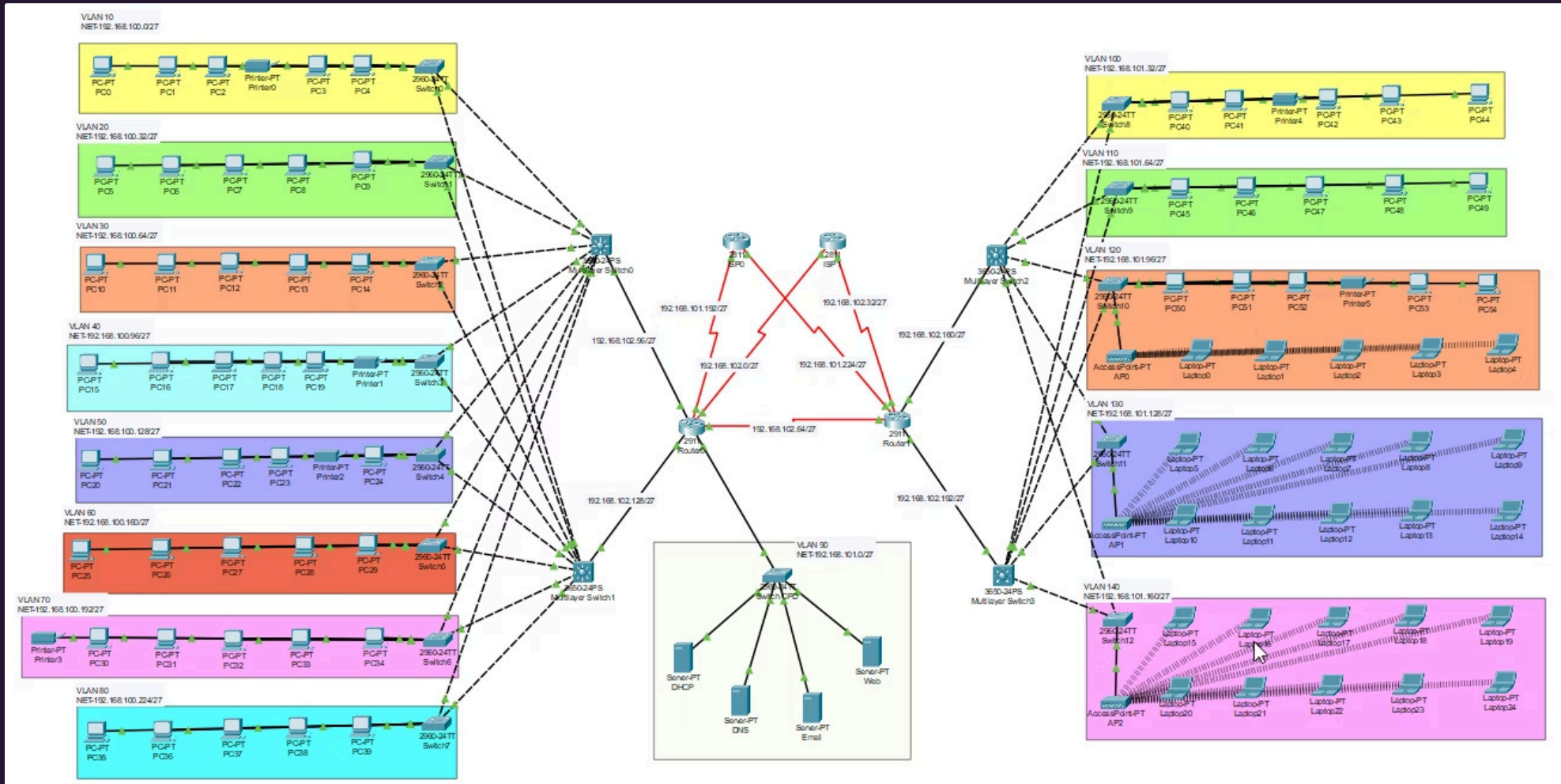
- Capa 2: Cisco C2960 – 24 puertos, VLAN, QoS
- Capa 3: Cisco C3650 – 24 puertos PoE+, seguridad avanzada, alto rendimiento

Software

- Sistema Operativo y Productividad: Windows 11 Pro, Microsoft 365 (Word, Excel, Teams, Outlook)
- Navegación y Comunicación: Chrome, Edge, Teams, Zoom
- Seguridad y Soporte: Windows Defender / ESET, AnyDesk / TeamViewer
- Gestión y Colaboración: OneDrive, SharePoint, Planner, Power Automate
- Otros: ERP (CONTPAQi / SAP B1), lectores PDF, herramientas de red (PRTG, UniFi)



Esquema de la Red y Distribución de Dispositivos



Configuración de la Infraestructura de Red



Configuración

- Se implementó un plan de subredes con máscara /27, permitiendo 30 hosts útiles por subred.
- Se definieron 23 subredes, cada una asociada a una VLAN específica, enlaces troncales, conexiones a ISP y dispositivos de capa 3.
- Este esquema mejora la segmentación, seguridad y eficiencia del direccionamiento IP.



Subredes

Subred #	Dirección de Subred	Rango Útil	Dirección de Broadcast	Asignado a
1	192.168.100.0/27	.1 – .30	192.168.100.31	VLAN 10
2	192.168.100.32/27	.33 – .62	192.168.100.63	VLAN 20
3	192.168.100.64/27	.65 – .94	192.168.100.95	VLAN 30
4	192.168.100.96/27	.97 – .126	192.168.100.127	VLAN 40
5	192.168.100.128/27	.129 – .158	192.168.100.159	VLAN 50
6	192.168.100.160/27	.161 – .190	192.168.100.191	VLAN 60
7	192.168.100.192/27	.193 – .222	192.168.100.223	VLAN 70
8	192.168.100.224/27	.225 – .254	192.168.100.255	VLAN 80
9	192.168.101.0/27	.1 – .30	192.168.101.31	VLAN 90 (CPD)
10	192.168.101.32/27	.33 – .62	192.168.101.63	VLAN 100
...

Fig. 2. Tabla de subredes



Infraestructura de Red

- Router Cisco 2911: Firewall, VLANs, VPN, administración centralizada
- Switches Cisco C2960 / C3650: Soporte para VLAN, QoS, PoE+, seguridad empresarial
- Segmentación mediante VLANs y subredes dedicadas (CPD, usuarios, servidores, etc.)

Instalación y Configuración del Servidor

Asignación de IP Estáticas para Servicios Críticos

Los servidores críticos de la red, como DHCP, DNS, y correo electrónico, fueron configurados con direcciones IP estáticas dentro del rango de la VLAN correspondiente al CPD.

Comunicación y Enrutamiento Centralizado

Esta asignación fija permite garantizar la estabilidad en la resolución de nombres, la entrega de servicios esenciales y la correcta comunicación con los dispositivos cliente. Además, se estableció una puerta de enlace predeterminada común para todos los servidores, asegurando el enrutamiento hacia el resto de la red.

Configuración del Servicio DHCP por VLAN

También, para facilitar la asignación automática de direcciones IP a los dispositivos finales, se habilitó el servicio DHCP en uno de los servidores. Se crearon múltiples pools de direcciones, cada uno asociado a una VLAN específica, con su respectivo rango de IP, máscara de subred, puerta de enlace y servidor DNS.



Gestión de Permisos y Políticas de Seguridad

Servidor Windows Server

La red cuenta con un servidor central que ejecuta Windows Server y gestiona cuentas de usuario, grupos y permisos de acceso.

1

2

Active Directory y GPO

Mediante Active Directory y Directivas de Grupo (GPO), se asignan automáticamente los permisos necesarios a cada usuario según su departamento o función.

Control de Acceso

Esto permite controlar el acceso a carpetas compartidas, impresoras y otros recursos de red, garantizando que cada empleado solo pueda acceder a la información relevante para su rol.

3

Políticas de Contraseñas

Se aplican políticas robustas de contraseñas, incluyendo requisitos de longitud, complejidad y renovación periódica.

Bloqueo de Sesiones

Se implementan restricciones de acceso fuera del horario laboral y bloqueo automático de sesiones inactivas.

Auditoría y Registro

Se habilitan registros detallados de accesos y modificaciones, facilitando la investigación de incidentes.

Conectividad y Acceso a Recursos Compartidos

Verificación de Conectividad y Servicios de Red

Para verificar la correcta conectividad entre los dispositivos de la red y el acceso a los recursos compartidos, podemos realizar pruebas utilizando el comando ping desde diferentes estaciones de trabajo hacia servidores, impresoras y otros equipos en distintas VLANs. Estas pruebas confirmaron que la comunicación entre departamentos es funcional y que los servicios como DHCP, DNS y compartición de archivos están disponibles.

```
C:\>
C:\>
C:\>ipconfig

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::200:CFF:FE1E:3cD7
    IPv6 Address . . . . .:
    IPv4 Address . . . . .: 192.168.100.9
    Subnet Mask . . . . .: 255.255.255.224
    Default Gateway . . . . .: 192.168.100.1

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .:
    IPv6 Address . . . . .:
    IPv4 Address . . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .:

C:\>ping 192.168.101.144

Pinging 192.168.101.144 with 32 bytes of data:

Reply from 192.168.101.144: bytes=32 time=56ms TTL=124
Reply from 192.168.101.144: bytes=32 time=35ms TTL=124
Reply from 192.168.101.144: bytes=32 time=3ms TTL=124
Reply from 192.168.101.144: bytes=32 time=21ms TTL=124

Ping statistics for 192.168.101.144:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 56ms, Average = 28ms

C:\>
```

Fig. 3. Pruebas de ping.

Simulación de Tráfico con Cisco Packet Tracer

Además, podemos utilizar el modo de simulación de Cisco Packet Tracer, lo que permite observar visualmente el flujo de paquetes y validar el comportamiento esperado del tráfico en la red.

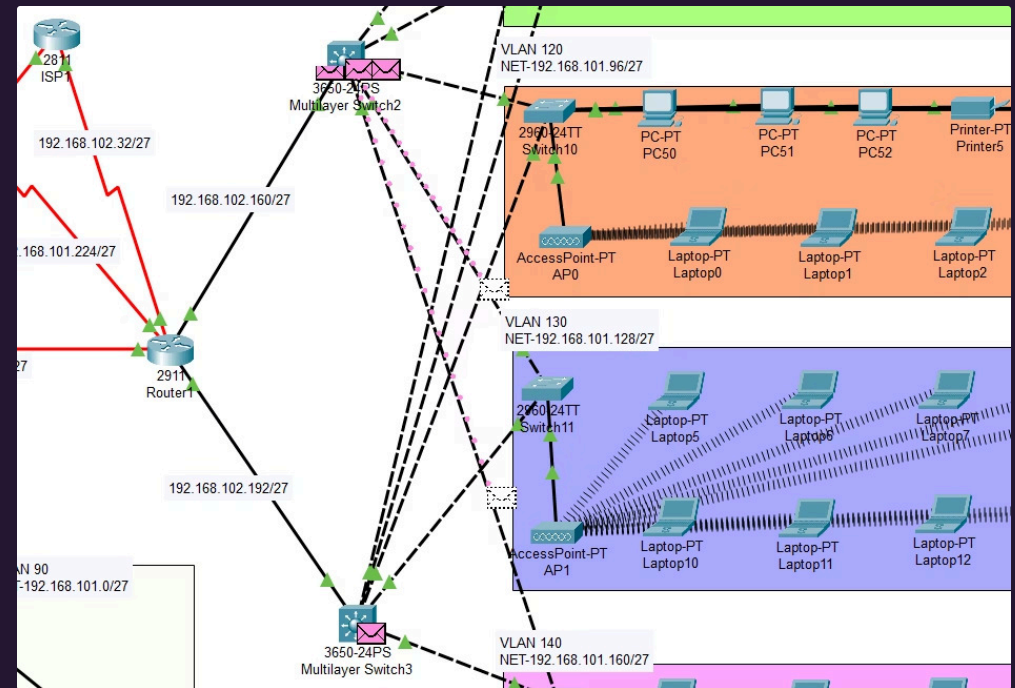


Fig. 4. Modo de simulación.



Conclusiones y Próximos Pasos

1 Implementación Efectiva

Adaptar infraestructura a necesidades actuales optimizando recursos disponibles.

2 Seguridad y Control

Aplicar políticas de acceso y monitoreo continuo para asegurar la integridad de la red.

3 Mantenimiento Continuo

Planificar actualizaciones y revisiones periódicas para garantizar disponibilidad y rendimiento.

4 Futuras Mejoras

Evaluar nuevas tecnologías para escalar y adaptar la red conforme crece la organización.