# **Características de la Red de Datos**

## **Tolerancia a Fallos**

### **Descripción**

La red está diseñada para garantizar alta disponibilidad y resiliencia ante fallos mediante las siguientes estrategias y tecnologías:

* **Redundancia de Enlaces:** Se implementan enlaces redundantes entre routers y switches para asegurar que, en caso de falla de un enlace, el tráfico pueda ser redirigido automáticamente a través de una ruta alternativa.
* **Protocolos de Enrutamiento Resilientes:** Se utilizan protocolos como OSPF (Open Shortest Path First) que permiten una rápida convergencia y redirección del tráfico en caso de fallos en la red.
* **Alta Disponibilidad (HA):** Los routers y switches clave están configurados en modos de alta disponibilidad, como HSRP (Hot Standby Router Protocol), para proporcionar conmutación por error sin interrupciones.

## **Escalabilidad**

### **Descripción**

La red está diseñada para crecer y adaptarse a las necesidades cambiantes, asegurando que nuevos dispositivos y segmentos de red puedan ser agregados sin interrupciones significativas:

* **Capacidad de Expansión:** La infraestructura permite la adición de nuevos switches y routers sin necesidad de grandes cambios en la configuración existente.
* **Segmentación de Red:** Se utiliza VLAN para segmentar la red, lo que facilita la adición de nuevos segmentos de red sin afectar la configuración de la red principal.
* **Enrutamiento Dinámico:** La implementación de protocolos de enrutamiento dinámico, como OSPF, facilita la adaptación de la red a cambios y expansiones de manera eficiente.

## **Calidad de Servicio (QoS)**

### **Descripción**

Se ha implementado QoS para garantizar un rendimiento óptimo de la red, priorizando el tráfico crítico y gestionando el ancho de banda de manera eficiente:

* **Prioridad de Tráfico:** Se utilizan políticas de QoS para priorizar el tráfico de voz y video sobre el tráfico menos crítico.
* **Control de Ancho de Banda:** Implementación de técnicas de gestión de ancho de banda para evitar la congestión y asegurar que las aplicaciones críticas tengan suficiente ancho de banda.
* **Marcado de Paquetes:** Los paquetes de datos se marcan según su importancia y tipo de servicio, permitiendo una gestión más eficiente del tráfico en la red.

## **Seguridad**

### **Descripción**

Se han implementado diversas medidas de seguridad para proteger la red contra amenazas internas y externas:

* **Firewalls:** Los firewalls controlan el acceso a la red, bloqueando el tráfico no autorizado y protegiendo contra ataques externos.
* **Sistemas de Detección de Intrusiones (IDS):** Monitorean el tráfico de red en busca de actividades sospechosas y potenciales amenazas.
* **Autenticación de Usuarios:** Se utiliza autenticación basada en roles y métodos de autenticación robustos para asegurar que solo usuarios autorizados puedan acceder a los recursos de la red.
* **Encriptación de Datos:** Los datos sensibles se cifran tanto en tránsito como en reposo para protegerlos contra accesos no autorizados.

## **Topología de la Red**

### **Descripción**

La topología de la red incluye la disposición física y lógica de los dispositivos de red, conexiones y segmentación en VLANs. A continuación, se presenta un diagrama detallado:

### **Componentes Clave**

* **Routers:** Router1 y Router2 conectados por un enlace punto a punto.
* **Switches:** Switch1 conectado a Router1 y Switch2 conectado a Router2.
* **PCs:** PC1 conectado a Switch1 y PC2 conectado a Switch2.
* **Segmentación:** Red 172.168.0.0/26 para Router2 y Switch2, Red 172.168.0.64/27 para Router1 y Switch1.

## **Protocolos y Tecnologías Utilizadas**

### **Lista y Descripción**

* **TCP/IP:** Protocolo fundamental para la comunicación en la red.
* **OSPF:** Protocolo de enrutamiento utilizado para la rápida convergencia y resiliencia.
* **VLAN:** Segmentación de la red para mejorar la gestión y seguridad.
* **VPN:** Protocolo para asegurar las conexiones remotas a la red.
* **HSRP:** Protocolo de redundancia para asegurar la alta disponibilidad de routers.

## **Pruebas y Validación**

### **Descripción**

Se han realizado varias pruebas para validar el funcionamiento de la red, asegurando su rendimiento y seguridad:

* **Pruebas de Conectividad:** Verificación de la conectividad entre todos los dispositivos de la red.
* **Pruebas de Rendimiento:** Evaluación del rendimiento de la red bajo diferentes cargas de tráfico.
* **Pruebas de Seguridad:** Simulaciones de ataques y pruebas de penetración para identificar vulnerabilidades.

## **Mantenimiento y Gestión de la Red**

### **Descripción**

Se han establecido prácticas de mantenimiento y gestión para monitorear y mantener la salud de la red:

* **Herramientas de Monitoreo:** Utilización de herramientas como Cisco Prime para la supervisión continua del rendimiento y estado de la red.
* **Políticas de Respaldo:** Programas regulares de respaldo de configuraciones y datos críticos.
* **Procedimientos de Recuperación:** Planes de recuperación ante desastres para asegurar la continuidad del servicio en caso de fallos mayores.

## **Conclusiones y Lecciones Aprendidas**

* **Lecciones Aprendidas:** La práctica de configurar y gestionar conexiones en dispositivos Cisco es importante para asegurar el correcto funcionamiento de redes de datos en entornos tanto pequeños como grandes. Es esencial tener un conocimiento sólido de los fundamentos de las redes, incluyendo la comprensión de cómo funcionan los protocolos de red, las direcciones IP, las subredes y los diferentes tipos de redes (LAN, WAN, etc.) Familiarizarse con los diferentes dispositivos Cisco (routers, switches, etc.) y sus funcionalidades es crucial. Cada dispositivo tiene su propio conjunto de comandos y configuraciones específicas que deben ser manejadas correctamente. Las habilidades deben abarcar las configuraciones básicas, como la asignación de direcciones IP y la configuración de interfaces.