31/05/2024

CARACTERISTICAS DE LA RED DE DATOS

SYSTEM ACADEMIC KO'S

Kaory Gissel Contreras Alvarez
Sofia Nava Cipriano
Odalis Bravo Depsa

CARACTERISTICAS DE LA RED DE DATOS:

1.- TOPOLOGÍA FÍSICA: Tenemos una red con una topología en “estrella”, en esta configuración, los dispositivos están conectados a un nodo central “enrutador”. Esta topología permite una fácil administración.

2.- Escalabilidad: La red que estamos haciendo esta diseñada para ser escalable, lo que significa que se pueden agregar nuevos dispositivos fácilmente.

3.- Velocidad y ancho de Banda: En este laboratorio se requiere una red de alta velocidad y ancho de banda para transferir grandes volúmenes de datos. La red esta diseñada con tecnología de fibra óptica y conmutadores de alta capacidad para garantizar velocidades de transferencia rápidas y un amplio ancho de banda para satisfacer a todos los alumnos.

4.- Costo: El o los switches pueden ser dispositivos costosos, mientras que los cables y otros componentes son relativamente económicos.

5.- Seguridad: En esta topología se aplica una variedad de medidas de seguridad para proteger los datos confidenciales y prevenir accesos no autorizados (secret password, password, service password encryption, etc).

6.- Compatibilidad: Existe compatibilidad, ya que se utilizan o se pueden utilizar diferentes dispositivos, como computadoras, enrutadores y switches.

7.- Tolerancia a Fallos: En esta red, se utilizan enrutadores y conmutadores con enrutamiento alternativo y conmutación por error.

8.- Facilidad de Uso: Esta red proporciona una interfaz de usuario intuitiva y sencilla para que nosotros podamos configurar y administrar la red de una manera fácil.

9.- Topología Lógica: Los datos se transmiten a través de la red por medio de ethernet y redes conmutadas (los dispositivos de red se comunican entre si a través de enlaces o conexiones punto a punto).

Características de la Red de Datos Explicadas a Detalle

Tolerancia a Fallos

Descripción:

Para garantizar la disponibilidad de la red en caso de fallos, se utilizan diversas estrategias y tecnologías que aseguran la continuidad del servicio. Algunas de estas estrategias incluyen:

- **Redundancia de Enlaces:** Implementación de múltiples enlaces físicos y lógicos entre dispositivos críticos para evitar puntos únicos de fallo. Por ejemplo, utilizar conexiones duales entre switches y routers.
- **Protocolos de Enrutamiento Resilientes:** Uso de protocolos de enrutamiento dinámico como OSPF (Open Shortest Path First) y BGP (Border Gateway Protocol) que reconfiguran automáticamente las rutas en caso de fallos en la red.
- **Alta Disponibilidad:** Configuración de dispositivos en pares de alta disponibilidad (HA), como firewalls y balanceadores de carga, que pueden tomar el control automáticamente si su par falla. Ejemplos incluyen HSRP (Hot Standby Router Protocol) y VRRP (Virtual Router Redundancy Protocol).

Escalabilidad

Detalles:

La red está diseñada para crecer y adaptarse a las necesidades cambiantes sin interrumpir el servicio. Las estrategias incluyen:

- **Diseño Modular:** Utilización de un diseño modular que permite agregar nuevos dispositivos y segmentos de red de manera sencilla.
- **Capacidad de Expansión:** Uso de switches y routers que soportan apilamiento y agregación de enlaces para aumentar la capacidad sin necesidad de reemplazar el hardware existente.
- **VLANs y Subnetting:** Implementación de VLANs (Virtual Local Area Networks) y subnetting para segmentar el tráfico y facilitar la expansión de la red.

Calidad de Servicio (QoS)

Explicación:

La implementación de QoS asegura un rendimiento óptimo de la red al priorizar el tráfico crítico y gestionar el ancho de banda eficientemente:

- **Clasificación del Tráfico:** Identificación y clasificación del tráfico basado en la prioridad, como voz, video y datos críticos.
- **Políticas de Prioridad:** Aplicación de políticas de prioridad que garantizan que el tráfico crítico tenga preferencia sobre el tráfico menos importante.
- **Gestión del Ancho de Banda:** Utilización de técnicas de gestión de ancho de banda como shaping y policing para asegurar que el uso de la red sea eficiente y justo.

Seguridad

Descripción:

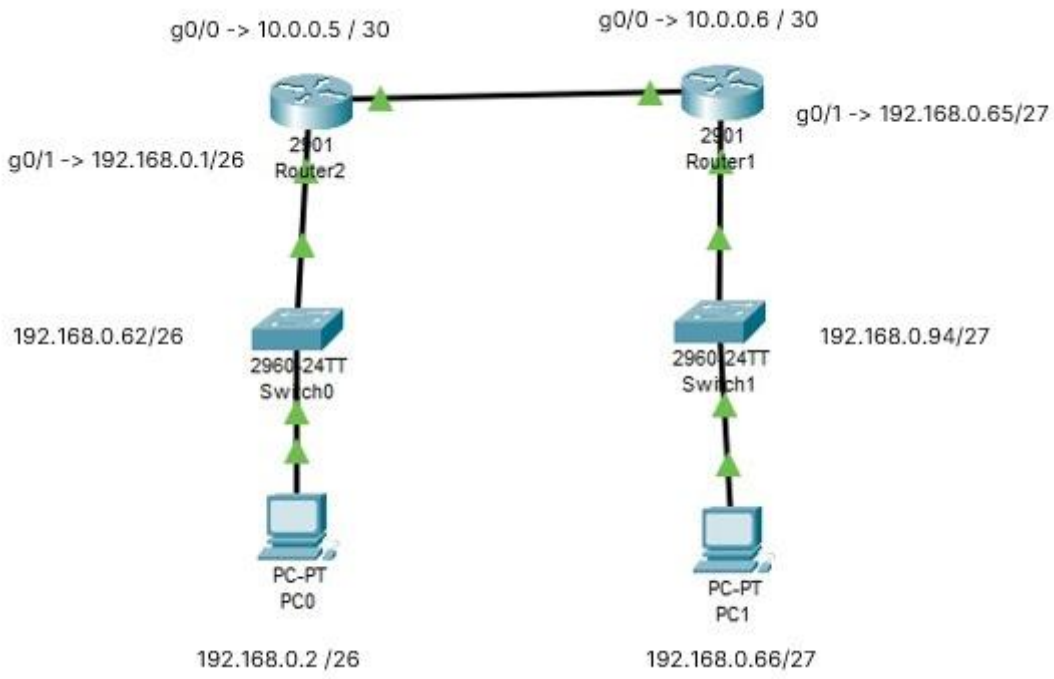
Para proteger la red contra amenazas internas y externas, se implementan varias medidas de seguridad:

- **Firewalls:** Configuración de firewalls en los perímetros de la red para controlar el tráfico entrante y saliente basado en políticas de seguridad.
- **Sistemas de Detección de Intrusiones (IDS) y Sistemas de Prevención de Intrusiones (IPS):** Monitoreo continuo del tráfico de red para detectar y prevenir actividades maliciosas.
- **Autenticación de Usuarios:** Uso de mecanismos de autenticación robustos como RADIUS y TACACS+ para controlar el acceso de los usuarios a la red.
- **Encriptación de Datos:** Implementación de protocolos de encriptación para proteger la confidencialidad e integridad de los datos en tránsito.

Topología de la Red

Diagrama:

Se incluye un diagrama detallado de la topología lógica de la red que muestra:



Disposición de dispositivos de red (switches, routers, pc).

Conexiones lógicas y enlaces redundantes.

Segmentación de la red en VLANs para organizar y aislar el tráfico.

Protocolos y Tecnologías Utilizadas

Lista:

- **TCP/IP:** Protocolo base para la comunicación en la red.
- **VLAN:** Tecnología para segmentar la red en dominios de broadcast más pequeños.

Cada uno de estos protocolos y tecnologías juega un papel crucial en el funcionamiento eficiente y seguro de la red.

Pruebas y Validación

Descripción:

Se realizaron diversas pruebas para asegurar el funcionamiento correcto de la red:

- **Pruebas de Conectividad:** Verificación de la conectividad entre dispositivos y segmentos de la red.
- **Pruebas de Rendimiento:** Evaluación del rendimiento de la red bajo diferentes cargas de tráfico.
- **Pruebas de Seguridad:** Simulación de ataques y validación de las políticas de seguridad implementadas.

Mantenimiento y Gestión de la Red

Detalles:

Las prácticas de mantenimiento y gestión de la red incluyen:

- **Políticas de Respaldo:** Implementación de políticas de respaldo regular de configuraciones y datos críticos.
- **Procedimientos de Recuperación ante Desastres:** Establecimiento de procedimientos claros para la recuperación de la red en caso de fallos mayores o desastres.

Conclusiones y Lecciones Aprendidas

Resumen:

Durante el desarrollo del proyecto, se obtuvieron las siguientes conclusiones y lecciones aprendidas:

- **Importancia de la Redundancia:** La implementación de redundancia es crucial para mantener la disponibilidad y fiabilidad de la red.
- **Flexibilidad en el Diseño:** Un diseño modular y escalable permite adaptarse rápidamente a las necesidades cambiantes.
- **Seguridad Proactiva:** La implementación de medidas de seguridad proactivas protege efectivamente contra una amplia gama de amenazas.
- **Documentación y Monitoreo:** La documentación detallada y el monitoreo continuo son esenciales para la gestión eficiente de la red y la resolución rápida de problemas.

Áreas de mejora identificadas incluyen la necesidad de actualizar periódicamente las políticas de seguridad y la capacitación continua del personal en las últimas tecnologías y amenazas.