Instituto Adventista Guanaja

Alumno: Andres Hernandez

Maestro: Jeovanny Barrera

Materia: Redes Informáticas

Grado: III BTPI

Asignación: Innovaciones en cables de red

Parcial: III Parcial

Fecha de entrega: 4/8/23

Tabla De Contenido

1.Portada…………………..

2.Tabla de contenido………………………

3.Introduccion……………………….

4.Investigacion……………………..

5.Conclusion…………………..

6.Opinion personal……………….

7.Bibliografia………………………

Introduccion

La configuración de una red empresarial es un proceso crítico que involucra la planificación, diseño, implementación y mantenimiento de una infraestructura de red para satisfacer las necesidades específicas de una organización. En la era digital actual, las redes empresariales son fundamentales para facilitar la comunicación interna, el intercambio de datos, el acceso a recursos compartidos y el soporte de aplicaciones clave para el funcionamiento eficiente de una empresa.

Configuración de una red empresarial

\*Topología de Red Estrella:\*

- \*Ventajas:\*

1. \*Centralización:\* Todos los datos pasan a través de un nodo central, facilitando el control y la gestión.

2. \*Fiabilidad:\* Si un dispositivo falla, no afecta al resto de la red.

3. \*Fácil Detección de Problemas:\* Las fallas son fáciles de detectar y diagnosticar.

- \*Desventajas:\*

1. \*Dependencia del Nodo Central:\* Si el nodo central falla, toda la red puede quedar inactiva.

2. \*Costo:\* Requiere más cableado que otras topologías.

\*Topología de Red Bus:\*

- \*Ventajas:\*

1. \*Simplicidad:\* Es fácil de instalar y requiere menos cableado.

2. \*Económica:\* Es más económica para redes pequeñas.

- \*Desventajas:\*

1. \*Colisiones:\* Los datos pueden colisionar en el bus, afectando la eficiencia.

2. \*Dificultad de Identificación de Problemas:\* Las fallas pueden ser difíciles de identificar y corregir.

\*Topología de Red Anillo:\*

- \*Ventajas:\*

1. \*Datos Unidireccionales:\* Los datos fluyen en una dirección, evitando colisiones.

2. \*Fácil Identificación de Fallas:\* Es fácil identificar el punto exacto de falla en el anillo.

- \*Desventajas:\*

1. \*Interrupción del Anillo:\* Si un nodo falla, todo el anillo puede quedar inactivo.

2. \*Complejidad en la Expansión:\* Agregar o quitar nodos puede ser complicado.

\*Topología de Red Malla:\*

- \*Ventajas:\*

1. \*Redundancia:\* Ofrece rutas alternativas para los datos, aumentando la confiabilidad.

2. \*Alta Tolerancia a Fallos:\* La red puede seguir funcionando incluso si algunos nodos fallan.

- \*Desventajas:\*

1. \*Costosa:\* Requiere una gran cantidad de cableado y dispositivos, siendo costosa de implementar.

2. \*Complejidad de Configuración:\* Configurar y mantener una red malla puede ser complejo y requerir habilidades técnicas avanzadas.

En un entorno empresarial, la elección de la topología de red dependerá de varios factores como el tamaño de la empresa, el presupuesto disponible, la necesidad de redundancia y la importancia de la tolerancia a fallos. La topología en estrella es común en redes pequeñas o medianas debido a su facilidad de administración, mientras que las redes malla son adecuadas para empresas grandes que requieren alta disponibilidad y tolerancia a fallos. La elección debe hacerse considerando cuidadosamente estos aspectos para asegurar un funcionamiento óptimo de la red empresarial.

\*Topología de Red Estrella:\*

- \*Ventajas:\*

1. \*Centralización:\* Todos los datos pasan a través de un nodo central, facilitando el control y la gestión.

2. \*Fiabilidad:\* Si un dispositivo falla, no afecta al resto de la red.

3. \*Fácil Detección de Problemas:\* Las fallas son fáciles de detectar y diagnosticar.

- \*Desventajas:\*

1. \*Dependencia del Nodo Central:\* Si el nodo central falla, toda la red puede quedar inactiva.

2. \*Costo:\* Requiere más cableado que otras topologías.

\*Topología de Red Bus:\*

- \*Ventajas:\*

1. \*Simplicidad:\* Es fácil de instalar y requiere menos cableado.

2. \*Económica:\* Es más económica para redes pequeñas.

- \*Desventajas:\*

1. \*Colisiones:\* Los datos pueden colisionar en el bus, afectando la eficiencia.

2. \*Dificultad de Identificación de Problemas:\* Las fallas pueden ser difíciles de identificar y corregir.

\*Topología de Red Anillo:\*

- \*Ventajas:\*

1. \*Datos Unidireccionales:\* Los datos fluyen en una dirección, evitando colisiones.

2. \*Fácil Identificación de Fallas:\* Es fácil identificar el punto exacto de falla en el anillo.

- \*Desventajas:\*

1. \*Interrupción del Anillo:\* Si un nodo falla, todo el anillo puede quedar inactivo.

2. \*Complejidad en la Expansión:\* Agregar o quitar nodos puede ser complicado.

\*Topología de Red Malla:\*

- \*Ventajas:\*

1. \*Redundancia:\* Ofrece rutas alternativas para los datos, aumentando la confiabilidad.

2. \*Alta Tolerancia a Fallos:\* La red puede seguir funcionando incluso si algunos nodos fallan.

- \*Desventajas:\*

1. \*Costosa:\* Requiere una gran cantidad de cableado y dispositivos, siendo costosa de implementar.

2. \*Complejidad de Configuración:\* Configurar y mantener una red malla puede ser complejo y requerir habilidades técnicas avanzadas.

En un entorno empresarial, la elección de la topología de red dependerá de varios factores como el tamaño de la empresa, el presupuesto disponible, la necesidad de redundancia y la importancia de la tolerancia a fallos. La topología en estrella es común en redes pequeñas o medianas debido a su facilidad de administración, mientras que las redes malla son adecuadas para empresas grandes que requieren alta disponibilidad y tolerancia a fallos. La elección debe hacerse considerando cuidadosamente estos aspectos para asegurar un funcionamiento óptimo de la red empresarial.

Dispositivos y componentes

\*1. Enrutadores:\*

Los enrutadores son dispositivos de red que conectan diferentes redes y dirigen el tráfico de datos entre ellas. Funcionan en la capa 3 (capa de red) del modelo OSI y toman decisiones basadas en direcciones IP para determinar la ruta más eficiente para enviar paquetes de datos. Los enrutadores también proporcionan funciones de seguridad, como el filtrado de paquetes y el control de acceso. Se configuran asignando direcciones IP, configurando tablas de enrutamiento y estableciendo políticas de seguridad.

\*2. Switches:\*

Los switches son dispositivos de capa 2 (capa de enlace de datos) que conectan múltiples dispositivos en una red local (LAN). A diferencia de los hubs, los switches pueden aprender las direcciones MAC de los dispositivos conectados y enviar datos solo al dispositivo de destino, lo que mejora la eficiencia de la red. Los switches se configuran para asignar VLANs (redes virtuales), implementar calidad de servicio (QoS) y administrar el tráfico de la red.

\*3. Firewalls:\*

Los firewalls son dispositivos de seguridad que protegen una red empresarial controlando el tráfico entrante y saliente. Pueden ser hardware o software y funcionan en las capas de red y aplicación del modelo OSI. Los firewalls pueden bloquear o permitir ciertos tipos de tráfico según reglas predefinidas, protegiendo la red contra amenazas como intrusiones, malware y ataques DDoS. Se configuran mediante reglas de filtrado, políticas de seguridad y configuraciones de proxy.

\*4. Puntos de Acceso Inalámbricos (APs):\*

Los puntos de acceso inalámbricos permiten que dispositivos como computadoras portátiles, teléfonos inteligentes y tabletas se conecten a una red empresarial de forma inalámbrica. Los APs se conectan a la red cableada y proporcionan acceso a través de tecnologías como Wi-Fi. Se configuran con SSID (identificador de conjunto de servicios), seguridad inalámbrica (por ejemplo, WPA2-PSK), y a menudo se implementan en VLANs separadas para una gestión y seguridad eficientes.

Configurar estos dispositivos implica acceder a sus interfaces de administración a través de direcciones IP específicas o software de gestión, donde se pueden realizar ajustes según las necesidades específicas de la red empresarial. Es importante seguir las mejores prácticas de seguridad al configurar estos dispositivos para proteger la red contra posibles amenazas.

Protocolos de enrutamiento

\*1. OSPF (Open Shortest Path First):\*

OSPF es un protocolo de enrutamiento de estado de enlace que calcula las rutas más cortas para enviar paquetes de datos en una red IP. Es un protocolo de enrutamiento dinámico y se utiliza en redes empresariales grandes y complejas. OSPF utiliza un algoritmo de estado de enlace (LSA) para determinar las rutas más eficientes y se adapta automáticamente a los cambios en la red, como enlaces caídos o nuevos enlaces.

\*2. BGP (Border Gateway Protocol):\*

BGP es un protocolo de enrutamiento de vector de distancia que se utiliza en internet y en redes grandes y heterogéneas. A diferencia de OSPF, que se enfoca en la topología interna de una red, BGP se utiliza para intercambiar información de enrutamiento entre sistemas autónomos (AS). BGP toma decisiones de enrutamiento basadas en múltiples atributos, como la política, la preferencia del camino y la métrica.

\*Comparación entre Enrutamiento Estático y Dinámico:\*

\*1. Enrutamiento Estático:\*

- \*Ventajas:\*

1. \*Simplicidad:\* Fácil de configurar y entender, especialmente en redes pequeñas y simples.

2. \*Seguridad:\* Al no enviar actualizaciones de enrutamiento, es menos vulnerable a ataques.

3. \*Previsibilidad:\* Las rutas son predefinidas y estables, lo que facilita la gestión del tráfico.

- \*Desventajas:\*

1. \*Escalabilidad:\* Puede volverse complejo y poco práctico en redes grandes y en constante cambio.

2. \*Adaptabilidad:\* No se ajusta automáticamente a cambios en la topología de la red, lo que requiere configuración manual en caso de cambios.

\*2. Enrutamiento Dinámico:\*

- \*Ventajas:\*

1. \*Adaptabilidad:\* Se ajusta automáticamente a cambios en la red, como enlaces caídos o nuevas conexiones.

2. \*Eficiencia:\* Encuentra rutas óptimas en función de las métricas y condiciones de red en tiempo real.

3. \*Escalabilidad:\* Es más adecuado para redes grandes y complejas, ya que maneja dinámicamente las actualizaciones de enrutamiento.

- \*Desventajas:\*

1. \*Complejidad:\* Requiere una configuración y gestión más complejas, especialmente en redes grandes.

2. \*Seguridad:\* Al intercambiar información de enrutamiento, puede ser vulnerable a ataques si no se asegura adecuadamente.

En resumen, el enrutamiento estático es adecuado para redes pequeñas y sencillas donde las rutas no cambian con frecuencia y se valora la simplicidad y la seguridad. Por otro lado, el enrutamiento dinámico, como OSPF y BGP, es esencial en redes empresariales grandes y complejas, ya que se adapta automáticamente a los cambios en la red, proporcionando eficiencia y escalabilidad. La elección entre enrutamiento estático y dinámico dependerá de las necesidades específicas y la complejidad de la red en cuestión.

Seguridad de red

Medidas de Seguridad en una Red Empresarial:\*

\*1. VLAN (Redes Virtuales):\*

Las VLANs son una forma de dividir una red física en segmentos lógicos, lo que permite separar dispositivos en grupos virtuales independientes. Esto proporciona seguridad al limitar el acceso de los usuarios a recursos específicos y segmentar el tráfico para reducir la superficie de ataque. Las VLANs ayudan a evitar que el tráfico no deseado llegue a ciertas partes de la red y facilitan la gestión de la seguridad.

\*2. Segmentación de Red:\*

La segmentación de red implica dividir una red en segmentos más pequeños y seguros para reducir el impacto en caso de una violación de seguridad. Los segmentos pueden estar basados en departamentos, funciones o niveles de seguridad. Al limitar la comunicación entre segmentos y aplicar políticas de seguridad específicas, la segmentación de red minimiza la propagación de amenazas y protege los datos sensibles.

\*3. Firewalls:\*

Los firewalls actúan como barreras de seguridad entre una red interna y el tráfico externo, filtrando el tráfico basándose en reglas predefinidas. Los firewalls pueden ser hardware o software y se configuran para bloquear o permitir ciertos tipos de tráfico. Los firewalls de próxima generación (NGFW) incluyen características como inspección profunda de paquetes, prevención de intrusiones y control de aplicaciones para ofrecer una protección más avanzada contra amenazas.

\*Establecimiento de Políticas de Seguridad:\*

1. \*Identificación de Activos y Vulnerabilidades:\* Antes de establecer políticas de seguridad, es crucial identificar los activos de la empresa y las posibles vulnerabilidades en la red. Esto incluye dispositivos, aplicaciones, datos y usuarios.

2. \*Definición de Políticas de Acceso:\* Establecer políticas claras de acceso que especifiquen quién tiene acceso a qué recursos. Esto incluye el principio de privilegios mínimos, que garantiza que los usuarios solo tengan acceso a los recursos necesarios para realizar sus tareas laborales.

3. \*Implementación de Controles de Acceso:\* Utilizar medidas como contraseñas fuertes, autenticación multifactor (MFA) y sistemas de gestión de identidades para controlar y proteger el acceso a sistemas y datos sensibles.

4. \*Actualizaciones y Parches:\* Mantener todos los sistemas, aplicaciones y dispositivos actualizados con los últimos parches de seguridad para protegerse contra vulnerabilidades conocidas.

5. \*Monitoreo y Respuesta:\* Establecer sistemas de monitoreo para detectar actividades sospechosas en la red. Tener un plan de respuesta a incidentes para abordar rápidamente cualquier violación de seguridad y minimizar el impacto.

6. \*Educación y Concientización:\* Educar a los empleados sobre las mejores prácticas de seguridad, como cómo identificar correos electrónicos de phishing y cómo proteger la información confidencial, es esencial para fortalecer la seguridad en toda la organización.

Al establecer y mantener políticas de seguridad bien definidas y utilizar medidas como VLAN, segmentación de red y firewalls, las empresas pueden crear una red empresarial segura y protegerse contra las amenazas cibernéticas.

Conclusión

En conclusión, asegurar una red empresarial implica una cuidadosa planificación, implementación y gestión de diversas medidas de seguridad. Tecnologías como VLANs, segmentación de red y firewalls son esenciales para proteger la red y los datos de la empresa contra amenazas cibernéticas. Establecer políticas de seguridad claras, aplicar controles de acceso rigurosos, mantener actualizados los sistemas y educar a los empleados son pasos fundamentales para mantener la integridad y confidencialidad de la información empresarial. En un mundo digital en constante evolución, la seguridad de la red empresarial es un esfuerzo continuo que requiere atención constante y adaptación a las últimas amenazas y tecnologías.

Opinión personal

asegurar una red empresarial implica la implementación de medidas de seguridad como VLANs, segmentación de red y firewalls. Estas tecnologías ayudan a dividir la red, limitar el acceso y filtrar el tráfico para proteger contra amenazas cibernéticas. Establecer políticas claras de acceso, mantener sistemas actualizados y educar a los empleados son pasos clave. La seguridad de la red es un esfuerzo continuo y esencial para proteger la integridad y confidencialidad de los datos empresariales en un entorno digital en constante cambio.