Descripción de los dispositivos y su funcionamiento en la red basadas en los requerimientos del trabajo:

Proveedor de Nube (Cloud): Esta es la entrada principal de la red, que representar la conexión a Internet proporcionado por un proveedor.

Router0: desempeña un papel crítico en nuestra infraestructura de red, actuando como el punto de entrada principal y el punto de control del tráfico entre la red interna y la nube proporcionada por nuestro proveedor de servicios de Internet (ISP). A continuación, se detallan algunas de las funciones y características clave del Router0:

Conexión a la Nube (Proveedor de Servicios de Internet): El Router0 representa el enlace principal entre nuestra red y la nube proporcionada por nuestro ISP. A través de esta conexión, se establece la puerta de entrada y salida de datos hacia y desde Internet, permitiéndonos acceder a servicios en la nube y recursos externos.

Enrutamiento del Tráfico: El Router0 es responsable de dirigir el tráfico de datos entre nuestra red local y la nube.

Firewall y Seguridad: Router0 actúa como un punto de control de seguridad al filtrar y controlar el tráfico entrante y saliente. Aplica políticas de seguridad que protegen nuestra red interna contra amenazas externas y restringe el tráfico no autorizado.

Administración y Configuración: Los administradores de red pueden acceder al Router0 para configurar y administrar sus funciones. Utilizan esta interfaz para ajustar la configuración de seguridad, las políticas de enrutamiento y otros aspectos de su funcionamiento.

Servidor: es una parte fundamental de nuestra red y desempeña un papel central en la provisión de servicios clave a otros dispositivos en la red. Algunas de las funciones esenciales que cumple el servidor incluyen:

Almacenamiento Centralizado de Archivos: El servidor actúa como un repositorio centralizado para el almacenamiento de archivos y datos críticos. Esto significa que los usuarios pueden acceder y compartir documentos, informes, archivos multimedia y otros recursos de manera eficiente desde un solo lugar. La centralización del almacenamiento simplifica la administración y la copia de seguridad de los datos, lo que garantiza la integridad y la disponibilidad de la información.

Hospedaje de Aplicaciones: El servidor aloja aplicaciones y servicios empresariales que son fundamentales para las operaciones. Esto puede

incluir aplicaciones de gestión de proyectos, sistemas de gestión de recursos empresariales (ERP), bases de datos y más. Al tener estas aplicaciones alojadas en un servidor dedicado, aseguramos un acceso rápido y confiable para los usuarios de la red.

Servicios de Correo Electrónico (SMTP y POP3): Hemos configurado el servidor para proporcionar servicios de correo electrónico utilizando los protocolos SMTP (Simple Mail Transfer Protocol) y POP3 (Post Office Protocol). Esto permite a nuestros empleados enviar y recibir correos electrónicos de manera eficiente, lo que es crucial para la comunicación interna y externa de la empresa.

Servicio de Transferencia de Archivos (FTP): Además, hemos habilitado un servicio FTP en el servidor para facilitar la transferencia de archivos dentro de la organización. Los usuarios pueden cargar y descargar archivos de manera segura, lo que es útil para compartir documentos, actualizaciones de software y otros recursos de manera eficiente.

Seguridad y Privacidad: Dado que el servidor almacena datos críticos y proporciona servicios clave, hemos implementado medidas de seguridad sólidas. Esto incluye el cifrado de las comunicaciones, la autenticación de usuarios, la copia de seguridad regular de datos y la supervisión constante para garantizar la integridad y la confidencialidad de la información.

Escalabilidad y Adaptabilidad: El servidor se ha configurado teniendo en cuenta la escalabilidad y la adaptabilidad. Esto significa que podemos expandir recursos de almacenamiento y capacidad de procesamiento a medida que crece la demanda de la empresa y las necesidades cambian con el tiempo.

En resumen, el servidor es el corazón de la red, proporcionando almacenamiento centralizado, servicios críticos y seguridad para nuestros datos y aplicaciones. Su papel es fundamental para el funcionamiento eficiente de la empresa y el cumplimiento de las necesidades de comunicación y colaboración de nuestros empleados y clientes.

PC de Terminal de Configuración: Cumple una función específica de administración y configuración que es esencial para el funcionamiento y el mantenimiento eficientes de la red. Algunos de los aspectos clave de su función incluyen:

Administración y Configuración de Dispositivos: Esta PC se dedica a la administración y configuración de los dispositivos de la red. Los administradores de red utilizan esta estación de trabajo para llevar a cabo tareas de configuración, supervisión y resolución de problemas en la red. Esto incluye la asignación de direcciones IP, la gestión de políticas de seguridad, la actualización de firmware y otras tareas de mantenimiento esenciales.

Control Centralizado: La PC de Terminal de Configuración actúa como un centro de control centralizado desde el cual se pueden gestionar y supervisar todos los dispositivos en la red. Esto facilita la administración eficiente de la infraestructura y garantiza que todos los dispositivos funcionen de manera coherente y cumplan con las políticas de seguridad y las necesidades operativas.

Resolución de Problemas: Cuando surgen problemas en la red, esta PC desempeña un papel crucial en la identificación y solución de problemas. Los técnicos y administradores pueden utilizar herramientas de diagnóstico y software de gestión para abordar problemas de conectividad, rendimiento o seguridad de manera efectiva.

Aplicación de Políticas de Seguridad: La PC de Terminal de Configuración se utiliza para aplicar y mantener políticas de seguridad en toda la red. Esto incluye la configuración de cortafuegos, listas de control de acceso (ACL) y otras medidas de seguridad para proteger los activos y los datos de la empresa.

Actualizaciones y Mejoras: Los dispositivos de la red, incluido el servidor y los routers, pueden requerir actualizaciones de firmware y mejoras periódicas. Esta PC se encarga de aplicar estas actualizaciones de manera regular para garantizar el rendimiento óptimo y la seguridad de los dispositivos.

Acceso Autorizado: Dado que tiene acceso a la configuración de dispositivos críticos, la PC de Terminal de Configuración se mantiene segura y solo se puede acceder a ella por personal autorizado. Se aplican medidas de autenticación y control de acceso para garantizar que solo las personas adecuadas tengan acceso a las funciones de administración y configuración.

Router1: Se utiliza para segmentar la red en diferentes subredes. Cada VLAN es como una red virtual independiente, y los dispositivos pertenecientes a estas VLAN pueden comunicarse entre sí como si estuvieran en una red física separada.

Además, se le configuraron listas de control de acceso que permite controlar qué tipo de tráfico está permitido o bloqueado entre dispositivos en una misma VLAN, garantizando la privacidad y la seguridad de la información crítica.

Switch: se conecta a Router1 y es esencial para segmentar la red en áreas o subredes específicas. Esto permite una administración más eficiente del tráfico y la seguridad al aislar dispositivos en segmentos separados de la red.

Hubs Estos se conectan al switch y se utilizan estratégicamente en nuestra red para reducir la cantidad de cableado que necesitamos conectar al

switch principal. En lugar de conectar cables individuales desde el switch a cada dispositivo en un área específica, utilizamos un hub en esa área. El hub actúa como un punto de conexión central para varios dispositivos en la misma área, lo que nos permite simplificar y organizar el cableado. De esta manera, logramos una distribución de cable más eficiente y ordenada en nuestra red, lo que facilita su administración y mantenimiento. Además, en la red, algunos dispositivos requieren un nivel adicional de seguridad y configuración, lo que hace necesario que estén conectados directamente al switch principal. Al conectarlos directamente al switch, tenemos un mayor control sobre su configuración y acceso. Esto nos permite implementar medidas de seguridad más estrictas y políticas de acceso específicas para garantizar que nadie más pueda ver ni acceder a estos dispositivos sin autorización. Esta configuración proporciona un nivel adicional de protección para los activos críticos y datos sensibles en la red.

Segunda Parte de la Red:

En la segunda parte de nuestra red empresarial, hemos implementado una topología similar que se conecta a la misma nube proporcionada por el proveedor de servicios de Internet (ISP). Detalles de los componentes clave de esta segunda parte:

Cable Módem: es el dispositivo que permite la conexión a la nube proporcionada por el ISP a través de la infraestructura de cable. Convierte las señales digitales de datos de la red en señales analógicas que pueden viajar a través de la línea de cable y viceversa. El cable módem es la puerta de entrada a Internet para esta parte de la red.

Router Inalámbrico: El router inalámbrico es un componente esencial que se encarga de dirigir el tráfico entre la red interna y la nube a través del cable módem. Además de proporcionar conectividad por cable, el router inalámbrico ofrece conectividad Wi-Fi, lo que permite que los dispositivos inalámbricos, como computadoras portátiles, teléfonos y tabletas, se conecten a la red de manera inalámbrica.

Switch2: es un conmutador de nivel de acceso que actúa como un punto central de conexión para dispositivos de esta parte de la red.

Hubs: Al igual que en la primera parte de la red, cada hub se conecta a Switch2 y actúa como un punto de conexión central para varios dispositivos en la misma área. La utilización de varios hubs permite simplificar y organizar el cableado en diferentes áreas y garantiza una distribución eficiente del cableado.

Reglas de Firewall Personalizadas: Hemos configurado reglas de firewall en nuestros dispositivos de red para permitir o bloquear el tráfico en función de las direcciones IP estáticas. Por ejemplo, hemos establecido reglas que permiten el acceso de ciertas direcciones IP a través de puertos

específicos, lo que garantiza que solo los dispositivos autorizados puedan acceder a servicios específicos.

Auditoría y Control de Acceso: Utilizamos registros de auditoría para realizar un seguimiento de la actividad de red y controlar quién accede a qué recursos. Las direcciones IP estáticas facilitan la identificación de dispositivos y usuarios y simplifican la implementación de políticas de acceso basadas en roles.

Políticas de Aislamiento: Hemos implementado políticas de aislamiento de red que restringen la comunicación entre dispositivos con direcciones IP estáticas. Esto asegura que solo los dispositivos específicos puedan comunicarse entre sí y evita la propagación de amenazas o accesos no deseados.

En resumen, la utilización de direcciones IP estáticas nos permite aplicar políticas de seguridad específicas y detalladas en nuestra red empresarial. Esto mejora la protección de nuestros activos críticos y datos sensibles, al tiempo que proporciona un mayor control sobre quién puede acceder a qué recursos. La segmentación de red, el control de acceso y las reglas de firewall personalizadas son algunas de las estrategias clave que empleamos para garantizar la seguridad en nuestra red.

Nuestra red representa una infraestructura sólida y bien diseñada que proporciona conectividad confiable, seguridad robusta y eficiencia en la administración de recursos. Cada componente de la red desempeña un papel crítico en su funcionamiento, y las configuraciones específicas han sido diseñadas para satisfacer las necesidades de la organización.

Lista de configuraciones del protocolo IPv4 para cada nodo, detallando si su asignación es estática o dinámica, y en este caso, servidor que la asigna.

Dispositivo Interfaz	Interfaz	Dirección IP	Conectar a
Nube	Eth6	No aplicable	Fa0/0
	Coax7	No aplicable	Port0
Router0	Fa0/0	192.168.1.1/24	Eth6
	Fa 0/1	10.0.0.1	Fa0
	Consola	No aplicable	RS232
	Ser 0/0/0	192.168.2.1/24	Serial 0/0
Servidor	Fa0	192.168.11.1	Fa01

Router1	Ser 0/0	192.168.2.1/24	Serial 0/0/0
Switch1	Fa0/1	192.168.3.1/24	Fa1/0
	Fa1/1	No aplicable	Fa0
	Fa2/1	No aplicable	Fa0
	Fa3/1	No aplicable	Fa0
	Fa4/1	No aplicable	Fa0
Hub Admin	Fa1/1	No aplicable	Fa0
	Fa1	192.168.3.5/24	Fa0
	Fa2	192.168.3.2/24	Fa0
	Fa3	192.168.3.3/24	Fa0
	Fa4	192.168.3.4/24	Fa0
	Fa5	192.168.3.6/24	Fa0
	Fa6	192.168.3.7/24	Fa0
	Fa7	192.168.3.8/24	Fa0
Hub Gerencia	Fa0	No aplicable	Fa/41
	Fa1	192.168.10.2	Fa0
	Fa2	192.168.10.3	Fa0
	Fa3	192.168.10.4	Fa0
Hub Ingeniería	Fa0	No aplicable	Fa2/1
	Fa1	192.168.4.2	Fa0
	Fa2	192.168.4.3	Fa0
	Fa3	192.168.4.4	Fa0
	Fa4	192.168.4.5	Fa0
	Fa5	192.168.4.5	Fa0
Hub Sala de Conferencia	Fa0	No aplicable	Fa0
	Fa1	192.168.5.2	Fa0
	Fa2	192.168.5.3	Fa0
Cable modem	Port0	No aplicable	Coaxial7
	Port1	No aplicable	Eth1
Router Inalámbrico	Eth1	No aplicable	Port1
	Internet	192.168.6.2	Fa1/1
Switch 2	Fa1	No aplicable	Fa1/1
	Fa2/1	No aplicable	Fa0
	Fa3/1	192.168.8.1	Fa0
	Fa4/1	No aplicable	Fa0
	Fa5/1	No aplicable	Fa0

Hub Programa de Producción	Fa5	No aplicable	Fa2/1
	Fa0	192.168.7.2	Fa0
	Fa1	192.168.7.3	Fa0
	Fa3	192.168.7.5	Fa0
	Fa4	192.168.7.5	Fa0
Hub Pañol	Fa0	No aplicable	Fa4/1
	Fa1	192.168.8.2	Fa0
	Fa2	192.168.8.3	Fa0
Hub Puesto de Operador CNC	Fa0	No aplicable	Fa5/1
	Fa0	192.168.10.2	Fa01
	Fa0	192.168.10.3	Fa2
	Fa0	192.168.10.4	Fa2
Hub Supervisión de taller	Fa5/1	No aplicable	Fa0
	Fa1	192.168.9.2	Fa0
	Fa2	192.168.9.3	Fa0
	Fa3	192.168.9.4	Fa0
	Fa4	192.168.9.5	Fa0

Direcciones IP:

Hemos optado por utilizar direcciones IP estáticas en áreas específicas con el propósito de aplicar políticas de seguridad detalladas. Algunas de las maneras en las que utilizamos direcciones IP estáticas para mejorar la seguridad incluyen:

Control de Acceso a Recursos Críticos: Hemos asignado direcciones IP estáticas a dispositivos que requieren acceso a recursos críticos de la empresa, como servidores de bases de datos, sistemas de almacenamiento y aplicaciones esenciales. Esta asignación permite que solo los dispositivos con direcciones IP específicas puedan acceder a estos recursos, reduciendo el riesgo de accesos no autorizados.

Segmentación de Red: Utilizamos direcciones IP estáticas para crear segmentos de red específicos para diferentes áreas o departamentos de la empresa. Cada segmento tiene su propia gama de direcciones IP estáticas, lo que facilita la administración y la aplicación de políticas de seguridad adaptadas a las necesidades de cada área. Esto nos permite aislar y proteger áreas críticas de la red.

Diagrama lógico de la red.