



UNLaM

Universidad Nacional de la Matanza

Escuela de formación continua

Licenciatura en Gestión de tecnología

Materia: Topología de Redes

Cátedra: 1317 - Comisión: 01-1700

Profesor: Rocco, Guillermo Horacio

Trabajo Práctico N.º 1

Diseño de Redes LAN / WAN

Integrantes

Alonso, Leandro

Aquino, Arami

Castillo, Emiliano

Chilon, Eduar

Vázquez, Tomás

Una empresa necesita reestructurar su infraestructura de red, por lo cual uds. han sido seleccionados por el departamento de sistemas para llevar a cabo el análisis y puesta en producción de esta.

La empresa está compuesta en cinco departamentos según su organigrama:

- Depto. de Dirección:
 - a) Se encuentra en el 4to piso.
 - b) Debe tener 8 puestos de trabajo.
 - c) Debe tener un servidor propietario.
 - d) Debe tener una impresora multifunción.

- Depto. de Programación:
 - a) Se encuentra 3er piso.
 - b) Debe tener 25 puestos de trabajo.
 - c) Debe tener un servidor propietario.
 - d) Debe tener una impresora multifunción.

- Depto. de Diseño:
 - a) Se encuentra 2do piso.
 - b) Debe tener 15 puestos de trabajo.
 - c) Debe tener un servidor propietario.
 - d) Debe tener una impresora multifunción.

- Depto. de Ventas:
 - a) Se encuentra 1er piso.
 - b) Debe tener 10 puestos de trabajo.
 - c) Debe tener un servidor propietario.
 - d) Debe tener una impresora multifunción.

- Depto. de Sistemas y Recepción:
 - a) Se encuentra en PB.
 - b) Debe tener 2 puestos de trabajo para Recepción.
 - c) Debe tener 5 puestos de trabajo para Sistemas en Gral.
 - d) Debe tener una impresora multifunción

Necesidades y consideraciones:

1. Conexión a internet para todos los puestos de trabajo.
2. Un server de gran capacidad en común para todos los departamentos él cual se utilizará como Servidor de archivos o "File Server".
3. A futuro la empresa tiene pensado en incrementar sus puestos de trabajo y servidores.
4. Actualmente tiene una línea de internet de 50 Mb conectada a un router en comodato por la empresa prestataria.
5. La empresa analizará la implementación de telefonía IP en cada uno de sus puestos por lo que se debe tener presente en el diseño.

1. Armar una topología acorde a las necesidades de la empresa:

Teniendo en cuenta las necesidades de la empresa y cada departamento, recomendaríamos una topología de estrella con subredes para cada uno. De esta manera, cada departamento tendría su propia red interna, pero estaría conectado a través de un switch central, el cual también recomendamos para que puedan tener acceso todos los departamentos al servidor de gran capacidad en común para todos utilizado como "File Server".

Creemos que la topología de estrella se adapta mejor por las siguientes razones,

- Facilita la administración de la red al tener un punto central de control, en este caso el switch central. Esto facilita la detección de problemas, la configuración y la implementación de nuevas tecnologías o cambios en la red.
 - Es escalable, como la empresa tiene pensado incrementar sus puestos de trabajo y servidores, agregar nuevos nodos a la red es más fácil y requiere menos configuración otras topologías.
 - Permite una distribución más eficiente del tráfico de red al tener un único punto central de conexión. Esto ayuda a minimizar la congestión de la red y a mejorar el rendimiento de los dispositivos conectados.
 - Puede ser más económica en términos de infraestructura y cableado, y con más facilidad en mantenimiento.
- a. **El Hardware necesario para armar la red. Router, switch, firewall, servidores, AP, racks, patcheras y otros accesorios necesarios de acuerdo a la topología elegida.**

Los hardware que se necesitan para la conexión red externa y distribución de conexión a la red interna serían:

- **Router**, necesario para tener conexión a internet y que distribuya el ancho de banda a todos los departamentos de la empresa.
- **Switch central**, para conectar todos los departamentos y permitir la comunicación entre ellos. También estará conectado a los servidores de archivos.
- **Firewall**, para la seguridad de la red.
- **Servidores**, se requiere un servidor de gran capacidad para almacenar los archivos compartidos de todos los departamentos. Además, cada departamento tendrá su propio servidor para sus necesidades específicas.
- **Access Points (AP)**, para brindar cobertura de red Wi-Fi en toda la oficina.
- **Patcheras**, para organizar todo el cableado.
- Como otro hardware puede ser antenas de WIFI.

b. **Estimar las bocas de red por cada puesto de trabajo.**

Por cada uno de los puestos de cada departamento, se estiman 2 bocas de la red, una para la PC y otra para la telefonía de IP.

- c. Diseñar la distribución de la red considerando el cableado estructurado, cableado eléctrico, ubicación de los servidores, impresoras y los dispositivos de Red.**

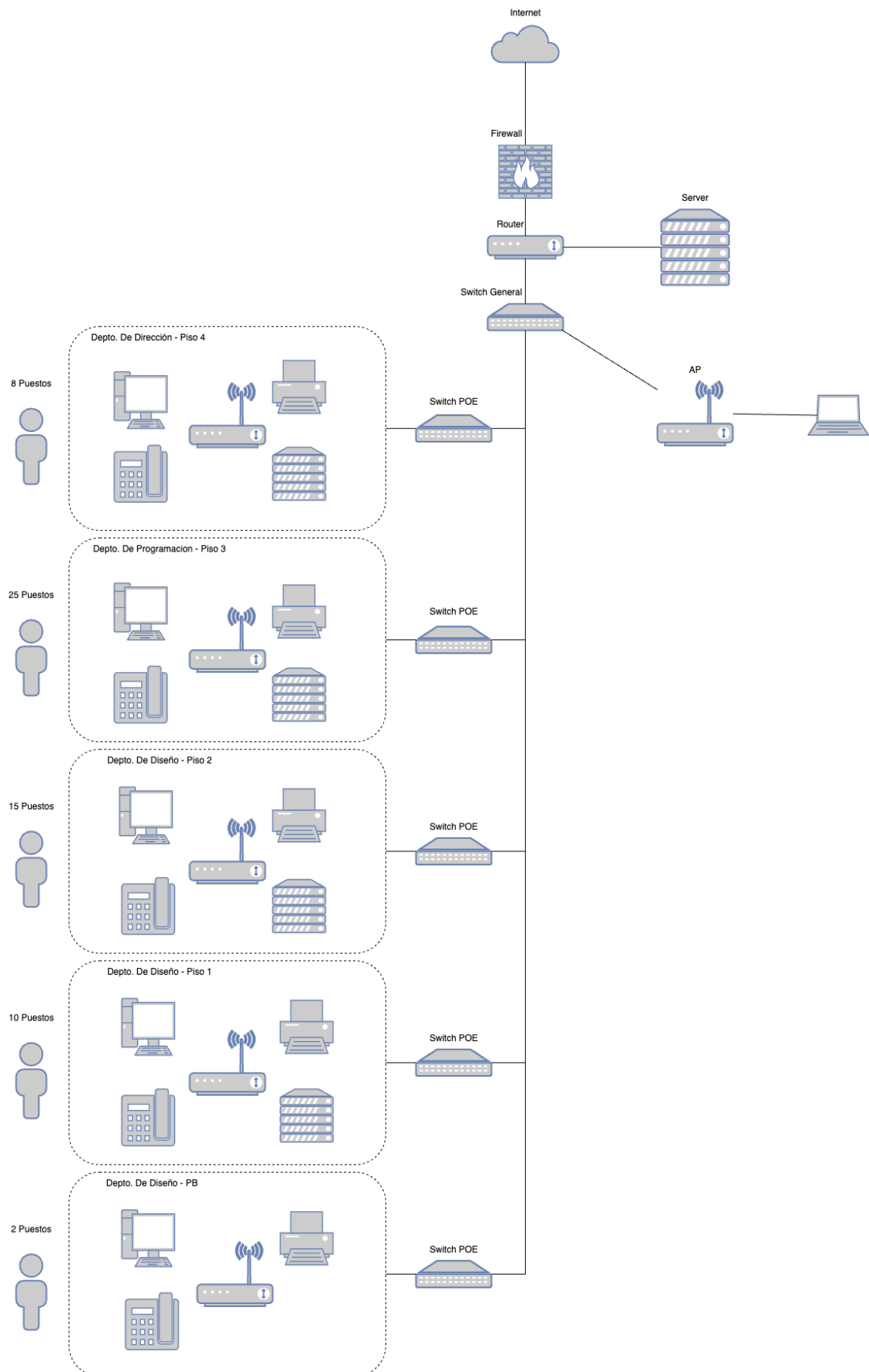
Para el diseño que estamos proponiendo, podría ser:

- Servidores cerca del equipo de soporte técnico y en un lugar seguro.
- Dispositivos de red en un rack de comunicaciones cerca de los equipos que van a conectar.
- Impresoras distribuidas estratégicamente en áreas de fácil acceso.
- Asegurar un cableado estructurado y eléctrico adecuado para mantener todo conectado y funcionando correctamente.

- d. Contemple bocas adicionales para las posibles salas de reunión en cada piso. Recomendable al menos 6 bocas cableadas por cada piso como mínimo.**

Consideramos 6 adicionales para cada piso, siempre conviene dejar una cantidad extra en zonas comunes para la empresa.

Además, se debe tener en cuenta cuantos puestos de trabajo se proyectan ampliar, considerando 2 bocas de red adicionales para cada uno de estos puestos futuros.



2. Evalúe si es necesario la instalación de switches Ethernet/PoE.

Dada la estructura y necesidades de esta empresa en particular, la instalación de switches Ethernet con PoE (Power over Ethernet) puede ser recomendado por:

- La empresa analiza la implementación de telefonía IP para cada puesto de trabajo, por ende, los switches Ethernet/PoE permitirían suministrar energía a estos dispositivos sin necesidad de una toma de corriente adicional.
- Es una opción que contribuye con la escalabilidad ya que los switches PoE permiten la instalación de nuevos dispositivos PoE en lugares donde puede ser difícil o costoso extender la alimentación eléctrica, lo que facilita la expansión de la red en el futuro.

3. Si fuera necesario para uds, implemente elementos de seguridad.

Para mejorar la seguridad de la red, sería necesario implementar algunos elementos tanto a nivel de hardware como de software:

Medidas de seguridad lógica:

- 1) **Firewall:** Este dispositivo protege la red interna de la empresa de amenazas externas. Filtra el tráfico de la red, bloquea el acceso no autorizado y evita ataques.
- 2) **Sistema de detección de intrusos (IDS):** Este software monitoriza la red y detecta actividades sospechosas.
- 3) **Antivirus y antimalware:** Se instalan en todos los equipos y servidores para proteger contra software malicioso.
- 4) **Proxy:** un servidor proxy actúa como intermediario entre el usuario y el servidor al que desea acceder. Un proxy puede ocultar la dirección IP del usuario, lo que proporciona cierto nivel de anonimato al navegar por la web.
- 5) **Autenticación de doble factor:** Esto agrega una capa extra de seguridad a la autenticación de usuario.
- 6) **VPN:** Para empleados que accedan a la red corporativa remotamente, es recomendable que lo hagan a través de una VPN para asegurar la transmisión de datos.

Medidas de seguridad física:

- 1) **Control de Acceso:** Se pueden usar llaves electrónicas, tarjetas de acceso, o sistemas biométricos.
- 2) **Videovigilancia:** Las cámaras de seguridad pueden desalentar a los delincuentes y proporcionar evidencia útil si se produce un incidente.
- 3) **Protección contra desastres:** Se pueden tener previsiones para proteger el equipo de eventos como incendios, inundaciones, etc.

7) **UPS:** Estos sistemas pueden proteger a los equipos contra descargas eléctricas y proporcionar electricidad en caso de un corte de luz.

8) **Auditorías de seguridad física:** Realizar auditorías periódicas puede ayudar a identificar y solucionar posibles problemas de seguridad física.

10) **Políticas de seguridad:** Cada empleado debe ser concientizado sobre las políticas de seguridad y el papel que desempeña en la seguridad de la red a fin de proteger información sensible.

4. Dentro del conocimiento y experiencia práctica entre los integrantes del grupo (si es que se tiene) analice el modelo de negocio que puede adoptar esta infraestructura de red (opciones de virtualización, tecnología Cloud, etc):

- Data center propio,
- Co-location,
- Hosting,
- Cloud computing.

1) **Data center propio:** Esta opción proporciona el mayor control sobre la infraestructura de red. Toda la gestión es interna, lo que puede ser útil si existen requisitos específicos de cumplimiento o seguridad. Es importante tener en cuenta que armar y mantener un data center propio puede ser costoso y requerirá personal técnico con estos conocimientos.

2) **Cloud computing:** Esta opción proporciona mayor flexibilidad, ya que los recursos pueden ser escalados hacia arriba o hacia abajo según las necesidades del negocio. Los costos suelen ser más bajos que en las demás opciones. La virtualización puede ayudar a reducir los costos de hardware y mejorar la eficiencia, mientras que la nube puede proporcionar flexibilidad y escalabilidad. Es importante entender el modelo de negocio de la empresa, las necesidades de los usuarios, la aplicación y la plataforma tecnológica para tomar la mejor decisión.

5. Justifique la respuesta del punto 4.

Recomendaciones:

- **Aplice sus conocimientos teniendo presente un costo imaginario “lógico/acorde” dependiendo el alcance de la empresa.**

Data Center Propio: Para almacenar datos críticos de la empresa y tener un control total sobre la seguridad de la infraestructura.

Creemos que, para una empresa en crecimiento, el **cloud computing** podría ser la opción más flexible y costo-efectiva. El costo se basa en el uso, por lo que puede escalar fácilmente a medida que la empresa crece, sin tener que invertir en hardware. Además, los proveedores de cloud computing manejan todo el mantenimiento, lo que libera al personal de IT para que se enfoque en proyectos que agreguen más valor a la empresa. Puede existir cierto riesgo y dependencia del proveedor, pero esto puede ser previsto con un contrato claro.

Un esquema de direccionamiento IP privado ayudaría para mantener la red organizada y segura. Esta decisión también debe considerar la privacidad y la seguridad de los datos de la empresa.