DATOS DE LA ACTIVIDAD							
No. de Actividad:	**2.9**	Avance Producto integrador	Seguridad en Infraestructura de TI				
Unidad:	Unidad 2: Configuración de seguridad en firewall, Switches, Routers y Access point						
Carrera:	Tgo. en Desarrollo de Software						
Materia	**SEGURIDAD EN ITI**					Clave	MPF3608DSO
Profesor:	Andrés Figueroa Flores						
Alumno:	Daniel Tejeda Saavedra					Registro:	17300288
Alumno:	David Alejandro López Torres					Registro:	17300155
Institución:	**Centro de Enseñanza Técnica Industrial plantel Colomos**						
Semestre:	8	Grupo:	D1	Período:	Feb-Jun 2021	Fecha:	07/05/2021
Compet. Genéricas	4.1, 4.5, 5.2, 5.5			Compet..		CP1-1	

Profesional

1. Objetivo(s) de la actividad

- Desarrollar por parte del alumno, el concepto integral de un proyecto informático relacionado con la propuesta de un sistema de red de computadoras con una implementación aplicando los conceptos de seguridad.

2. Introducción

Muchas empresas necesitan implementar mejoras en sus sistemas de seguridad informática, mejorar la seguridad de la empresa reestructurar las políticas, infraestructura aplicando los conceptos de seguridad.

Instrucciones:

- Con tu equipo previamente formado en 1er Parcial: En base a la propuesta de solución y a las políticas de red presentadas en el 1er Parcial, hacer el planteamiento en Packet Tracer de dicha propuesta. Hacer un diseño redundante (de preferencia una topología de anillo).
- Integrar los elementos (equipos, topología, tabla de Direccionamiento IP) para la actualización de la red con las consideraciones de mejora propuestas.
- El diseño de direcciones IP debe considerar el diseño VLSM, a partir de la red 172.XX.0.0/10 (XX = a los últimos dos dígitos del registro de algún integrante del equipo) para las PC de las sucursales y a partir la red 10.10.0.0/24 para conectar los routers de las 3 sucursales.

- En el documento hacer un listado de equipos y dar una explicación de los equipos seleccionados y de la topología propuesta.

FASE 1

Resumen de las características de la empresa:

Nombre Empresa: Dulces Nacionales Mexicanos

Locación: Occidente del país, Corporativo en Gdl, Producción en lagos de moreno y Cd Guzmán. **Sistema**

Telefónico: PBX

Red:

- 270 computadoras (frecuentes interrupciones),
- 6 impresoras (4 laser y 2 matriz de puntos) con alta impresión personal y no institucional. Cableado no estructurado.
- 12 switches de 24 puertos interconectados.
- Sin políticas de empleo de red y computo (se instalan programas de todo tipo sin control)
- Acceso a internet por enlace privado (DS0), renta mensual de 1,500,000.
- Sin restricciones de acceso a internet (Productividad baja de los ejecutivos).
- Tienen red inalámbrica, pero no está administrada y notan que seguido baja el desempeño o no se pueden conectar.
- En las plantas tienen redes con 17 y 24 computadoras respectivamente.
- La alimentación eléctrica es particularmente inestable en época de lluvias.
- Tienen tierra física y NoBreaks, pero ha sucedido que se interrumpe la energía eléctrica y los servers se han llegado a apagar.
- No cuentan con sistemas de prevención de intrusos ni alguna protección similar

Departamento Sistemas: Solicitan aumentar su equipo de 5 personas (1 gerente, 1 administrador de la red y 3 operadores, a 2 personas más). el cual no se da abasto resolviendo la problemática de la operación diaria. Se conectan a Internet por línea telefónica y el cableado es muy inestable y lento.

- El Gerente de sistemas, que no tiene una formación en informática, sino en contabilidad, solicita asesoría profesional para proponer un proyecto informático que les ayude a resolver la problemática, aumentar la productividad, reducir los gastos de operación, contar con una estructura de administración, seguridad y mejorar la comunicación tanto entre las plantas como con sus clientes.

Departamento de Producción: Requiere un servidor para instalar un programa de planeación de la producción que recientemente se lo ha presentado.

Departamento RRHH y Administración: RRHH y Administración requieren comunicarse con los departamentos homónimos en las plantas de manera frecuente y segura para la transmisión y uso de archivos confidenciales debido a un proyecto de reestructuración y adopción de la norma ISO/9000 en administración y producción.

Corporativo: La facturación mensual del corporativo asciende en promedio a $55,0000.00 y la tendencia es a aumentar. Los clientes han empezado a quejarse de que cada vez es más difícil comunicarse a ventas para la puesta de pedidos.

Evento: Infección masiva de computadoras por un virus provocando 2 días sin uso del equipo y un pico en el trabajo regular del equipo de sistemas.

Problemática:

1.- Los componentes de la red:

Los componentes de la red son una parte vital, el resumen menciona que el cableado no es estructurado lo cual puede complicar cualquier intento de mantenimiento y escalabilidad de la red. A si mismo es importante considerar que la elección del tipo de cable utilizado para el servicio de internet sea el correcto y congruente con el resto de los dispositivos de interconexión en la red pues esto podría causar cuellos de botella que finalmente se manifestarían como “lento internet” o “no poderse conectar a internet”. Así mismo otra razón por la que es importante observar la congruencia entre dispositivos de la red se debe al gran gasto en un servicio de internet que esta pagando la empresa (1,500,000 mensuales), no tendría caso pagar tanto dinero por un servicio de internet “de alta velocidad” si los dispositivos de interconexión no pueden sostener esta latencia. Por otro lado, es claro que el servidor no posee los cuidados y almacenamiento correcto que debería. No existe un servidor de respaldo que pueda entrar en caso de falla del servidor.

2.- Políticas de la red y administración de la red:

Es claro que la red no está administrada correctamente, así mismo no existen políticas que aseguren y promuevan su uso correcto. Las impresoras no poseen ningún tipo de restricción de uso y tienen un mayor uso personal que institucional. Las computadoras tampoco poseen restricción de ningún tipo, los empleados tienen control sobre los recursos de los ordenadores y pueden instalar programas sin autorización de supervisores. La información a lo largo de la red no se encuentra centralizada menos aun administrada de forma correcta. La red no posee ningún tipo de servicio instalado de forma que se pueda agilizar la gestión de información y la comunicación entre empleados por medio de esta.

3.- El personal

El equipo de sistemas no es suficiente para dar abasto con las necesidades en materia de red y administración de la red. Mas aun el personal no se encuentra capacitado para dar la atención, mantenimiento y administración correcta a la red. Dado la falta de infraestructura el personal de este departamento no tiene los medios para realizar la debida supervisión de la red.

4.- Locación

Las plantas de la organización están en distintos puntos geográficos de modo que para realizar una correcta comunicación entre estas es necesario establecer un tipo específico de red. Sin embargo, si la red no está administrada de forma local correctamente dudo mucho que lo esté en un nivel más alto. Por tanto, a los problemas de comunicación entre departamentos se añade el factor de la distancia.

5.- Software

La red no posee ningún tipo de software que ayude a la administración de esta, la falta de un programa que pueda arrojar datos de utilidad sobre el rendimiento de la red vuelve más difícil la tarea del supervisor. El servidor no está configurado a nivel de software de forma correcta para proporcionar los servicios que la empresa necesita que dé. Los dispositivos de interconexión no se encuentran configurados a nivel de software de forma correcta tanto en materia de funcionalidad como de seguridad básica. Las computadoras no poseen ningún tipo de software de protección antimalware. La configuración de seguridad de internet (sobre el ISP) es mínima, lo que puede propiciar a intrusos “colgándose” de este servicio.

Reflexión

Resolver problemáticas de carácter empresarial nos ayuda a conocer en que clases de contexto podemos aplicar los conceptos de seguridad en infraestructura en tecnologías de la información, podemos ver como tal no encontramos los conceptos vistos explícitamente, debemos analizar con cuidado la situación para encontrar las causas del problema y relacionarlas con los conceptos teóricos conocidos. Por tanto, me parece una importante practica pues esto es lo que más se puede asemejar a lo que veremos en el ámbito laboral.

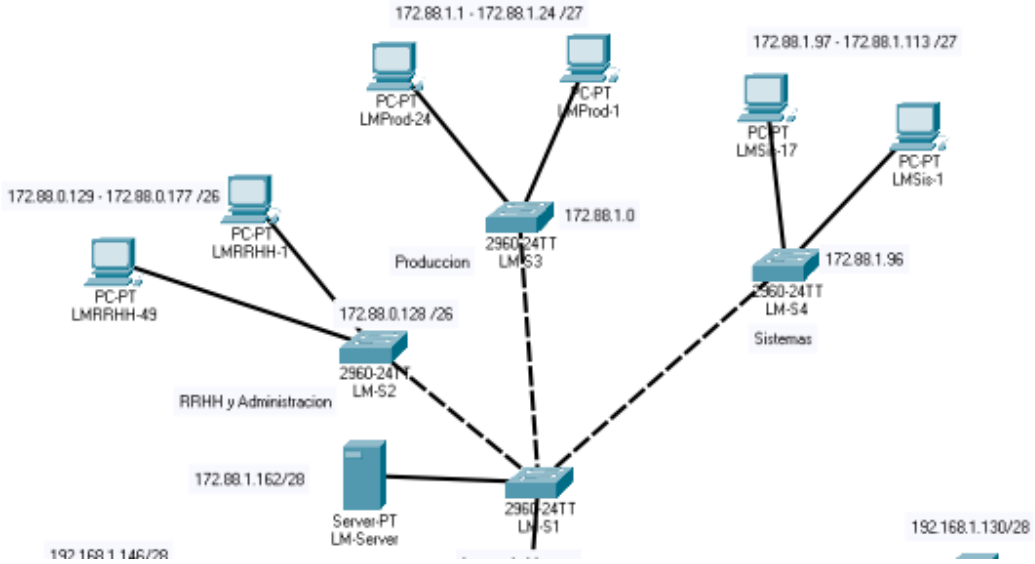
FASE 2

De acuerdo con el texto que plantea la problemática existen un total de 270 computadoras entre las 3 sucursales. Además, indica que en las plantas se tienen 14 y 27 computadoras respectivamente. Haciendo la división por sucursales existen 90 computadoras por sucursal (i.e. 270/3). Se dejaron 14 para la división de sistemas, 27 para la de producción y el resto quedaran entre recursos humanos y administración. Cada sucursal posera un servidor para administrar su red de forma local independientemente y mantener la información centralizada. Además, el hecho de tener 3 servidores nos ayuda en el sentido de que podemos realizar copias de la información de cada una de las sucursales en cada servidor (información redundante). Esto evitara que perdamos completamente la información en caso de que estos se apaguen de repente o haya un ataque a la red (situación que se menciona en el texto ha pasado).

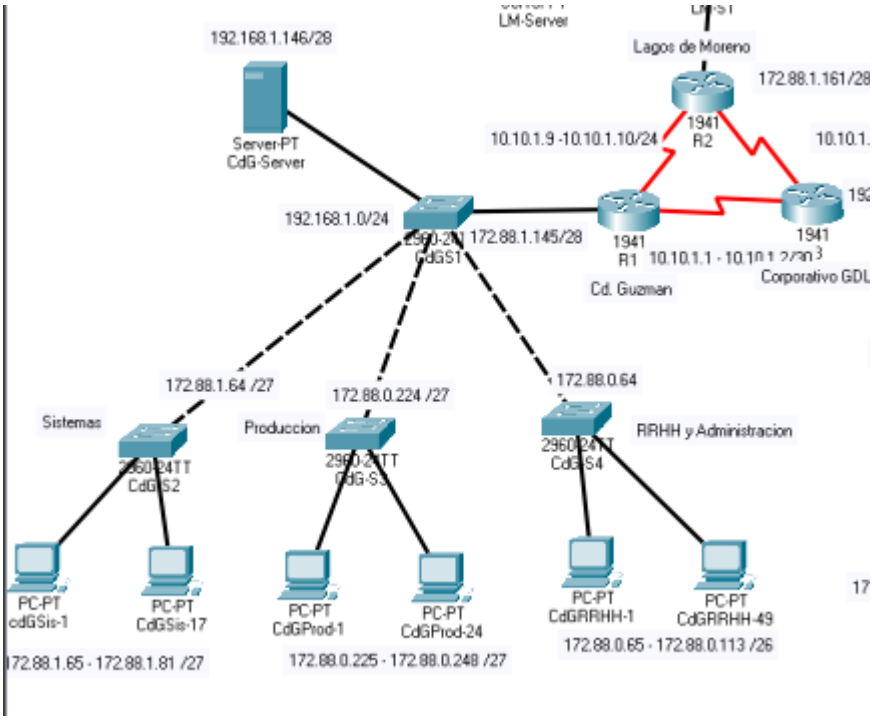
En el texto se menciona que los departamentos de recursos humanos y administración intercambian mucha información (en el texto como tal no se menciona cuantos ordenadores hay en cada departamento). Por tanto, con tal de volver eficiente la comunicación entre ellos se les dejara en una misma subred.

Se decidió implementar la siguiente topología con redundancia:

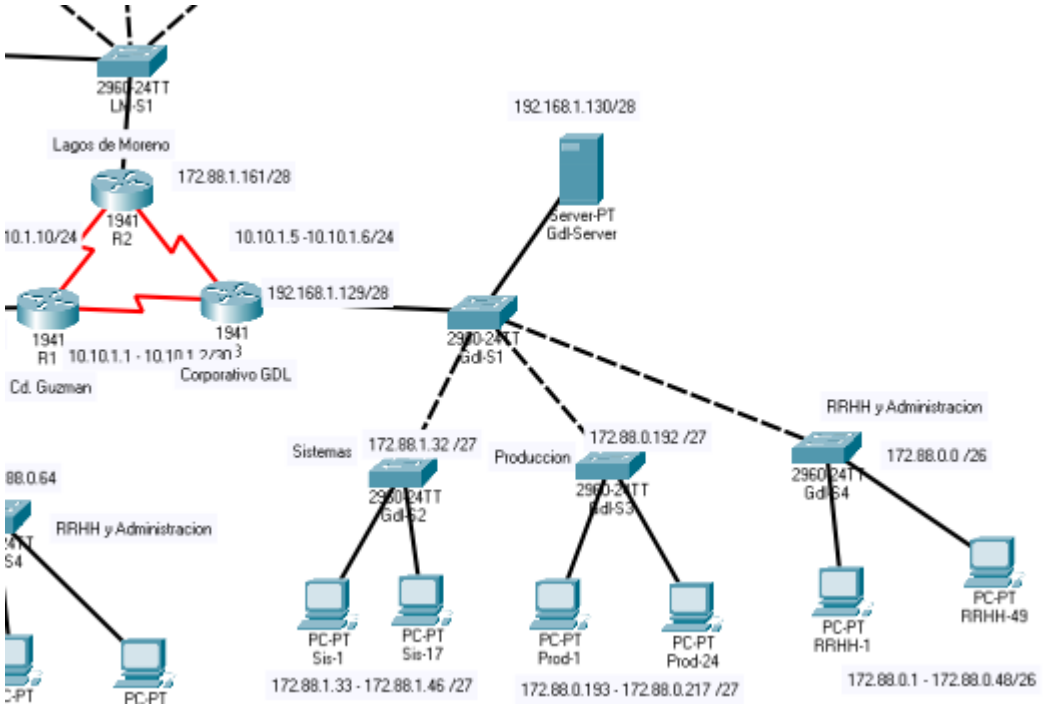
Parte superior:



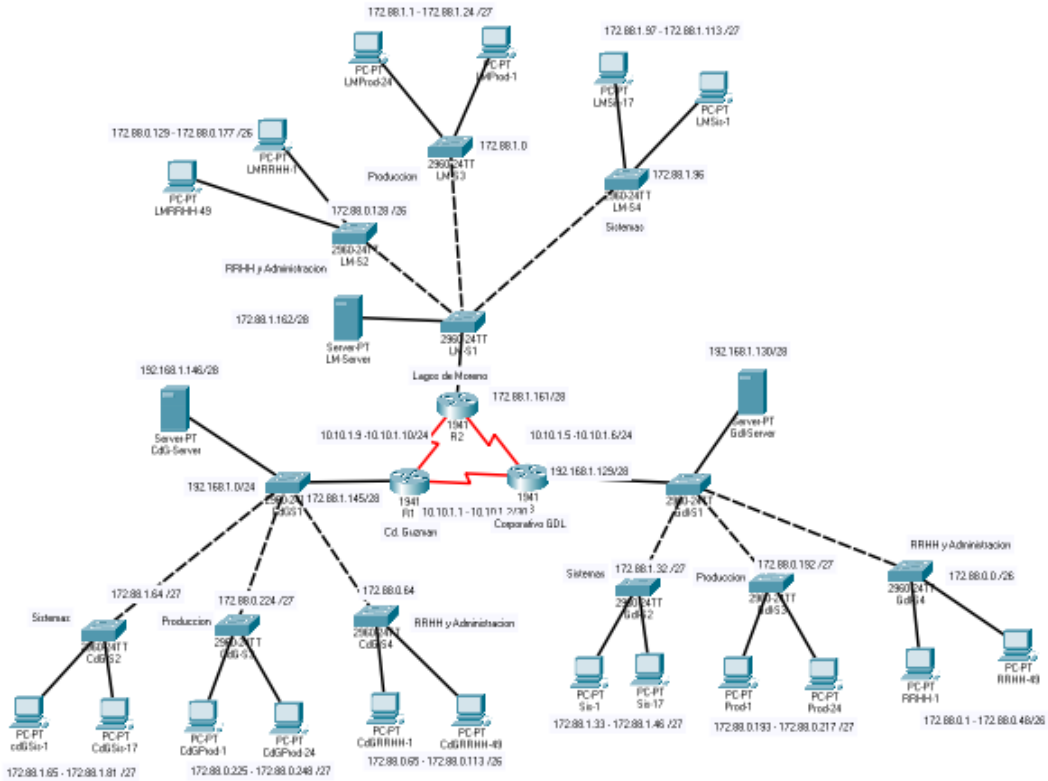
Lado Izquierdo:



Lado Derecho:



Vista Completa:



Subdivisión de la Red de Computadoras

Nombre	Hosts necesitados	Hosts Disponibles	Dirección Red	Slash	Mascara	Rango	Broadcast	Wildcard
GdlRRH y Admin	49	62	172.0.0.0	/26	255.255.255.192	172.88.0.1 - 172.88.0.62	172.0.0.63	0.0.0.63
Cd.G.RRH y Admin	49	62	172.0.0.64	/26	255.255.255.192	172.88.0.65 - 172.88.0.126	172.0.0.127	0.0.0.63
LM. RRH y Admin	49	62	172.0.0.128	/26	255.255.255.192	172.88.0.129 - 172.88.0.190	172.0.0.191	0.0.0.63
Gdl. Prod	24	30	172.0.0.192	/27	255.255.255.224	172.88.0.193 - 172.88.0.222	172.0.0.223	0.0.0.31
Cd. G. Prod	24	30	172.0.0.224	/27	255.255.255.224	172.0.0.225 - 172.0.0.254	172.0.0.255	0.0.0.31
LM. Prod	24	30	172.0.1.0	/27	255.255.255.224	172.0.1.1 - 172.0.1.30	172.0.1.31	0.0.0.31
Gdl. Sis	17	30	172.0.1.32	/27	255.255.255.224	172.0.1.33 - 172.0.1.62	172.0.1.63	0.0.0.31
Cd. G. Sis	17	30	172.0.1.64	/27	255.255.255.224	172.0.1.65 - 172.0.1.94	172.0.1.95	0.0.0.31
LM. Sis	17	30	172.0.1.96	/27	255.255.255.224	172.0.1.97 - 172.0.1.126	172.0.1.127	0.0.0.31
Gdl. Server	10	14	172.0.1.128	/28	255.255.255.240	172.0.1.129 - 172.0.1.142	172.0.1.143	0.0.0.15

Cd. G. Server	10	14	172.0.1.144	/28	255.255.255.240	172.0.1.145 - 172.0.1.158	172.0.1.159	0.0.0.15
LM. Server	10	14	172.0.1.160	/28	255.255.255.240	172.0.1.161 - 172.0.1.174	172.0.1.175	0.0.0.15

Distribución de las conexiones WAN

Nombre	Hosts necesitados	Hosts Disponibles	Hosts Sin usar	Network Address	Slash	Mascara	Rango	Broadcast	Wildcard
Host2	2	2	0	10.10.0.4	/30	255.255.255.252	10.10.0.5 - 10.10.0.6	10.10.0.7	0.0.0.3
Host3	2	2	0	10.10.0.8	/30	255.255.255.252	10.10.0.9 - 10.10.0.10	10.10.0.11	0.0.0.3
Host1	2	2	0	10.10.0.0	/30	255.255.255.252	10.10.0.1 - 10.10.0.2	10.10.0.3	0.0.0.3

Tabla de Direcciones

Device	Interface	IP Address	Default Gateway
RGdl	G0/1	172.88.1.129	N/A
	S0/0/0 (DCE)	10.10.1.2	N/A
	S0/0/1	10.10.1.6	
RCd.G.	G0/1	172.88.1.145	N/A
	S0/0/0	10.10.1.9	N/A
	S0/0/1 (DCE)	10.10.1.1	N/A
RLM.	G0/0	172.88.1.161	N/A
	S0/0/1	10.10.1.5	N/A
	S0/0/0	10.10.1.10	
Server Gdl	NIC	172.88.1.130	172.88.1.129
Server CdG.	NIC	172.88.1.146	172.88.1.145
Server LM	NIC	172.88.1.162	172.168.1.161
GdlSis1 – GdlSis17	NIC	172.88.1.33 - 172.88.1.46	172.88.1.129
Prod1 – GdlProd24	NIC	172.88.0.193- 172.88.0.217	172.88.1.129
GdlRRHH1 – GdlRRHH49	NIC	172.88.0.1	172.88.1.129
CdGSis1 – CdGSis17	NIC	172.88.1.65 – 172.88.1.81	172.88.1.145
CdGProd1 – CdGProd24	NIC	172.88.0.225 - 172.88.0.248	172.88.1.145
CdGRRHH1 – CdGRRHH49	NIC	172.88.0.65 - 172.88.0.113	172.88.1.145
LMSis1 – LMSis17	NIC	172.88.1.97 – 172.88.1.113	172.88.1.161
LMProd1 – LMProd24	NIC	172.88.1.1 - 172.88.1.24	172.88.1.161
LMRRHH1 – LMRRHH49	NIC	172.88.0.129 - 172.88.0.177	172.88.1.161

Reflexión:

Daniel

Es complicado tratar de hacer un esquema topológico, así como la subdivisión de redes cuando la información sobre los recursos y máquinas de esta es ambigua. Esto deja en claro el hecho de que al preguntar o entrevistar al cliente sobre el estado de la red debemos extraer la información necesaria como para saber con cuantos hosts vamos a trabajar, así como a que departamento pertenece cada uno de ellos, esto debe quedar muy claro para quien diseña la topología, así como el que elabora la repartición de IP's.

David

Con el desarrollo de esta nueva etapa del proyecto se afrontaron los diferentes problemas que pueden presentarse al diseñar una distribución topológica de la red de acuerdo con los requerimientos del cliente que, en principio, podrían caer en ambigüedades que pueden volverse deficiencias e ineficiencias en la red final. Una participación y comunicación directa con el cliente durante el proceso de diseño antes de realizar alguna implementación en los dispositivos de red es vital para generar un diseño que pueda satisfacer cada una de las necesidades del cliente y permite al diseñador tomar las mejores decisiones parala distribución de este.

Bibliografía:

--