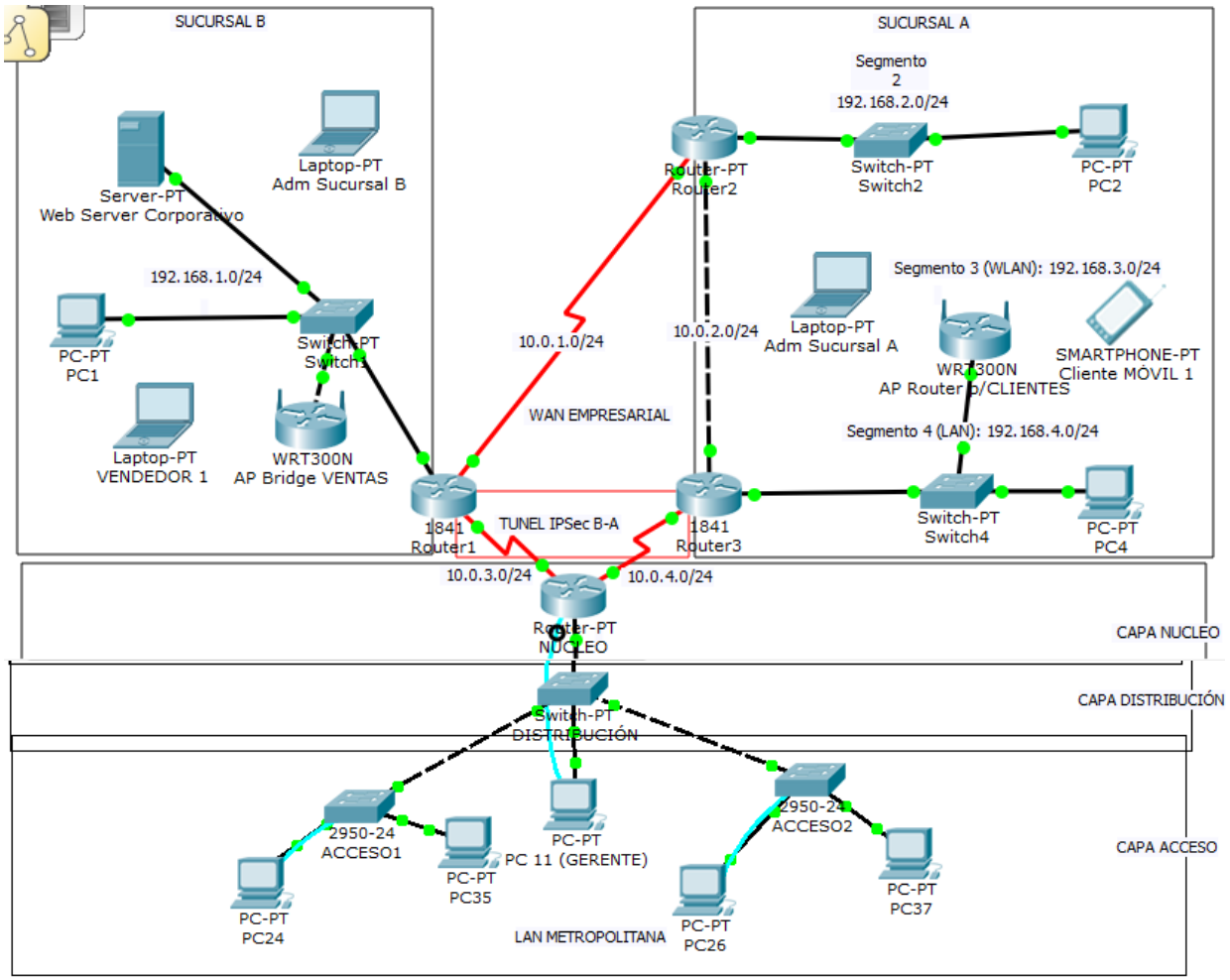
2018 - EJERCICIO INTEGRADOR DE AUTOEVALUACIÓN

OBJETIVO DEL EJERCICIO

Integrar el conocimiento práctico del alumno, de manera individual y autónoma, en la implementación de funciones y servicios de una red empresarial tanto LAN como WAN, en ambiente de laboratorio con simulador, poniendo en práctica habilidades en:

- Aplicación de normas de cableado estructurado e implementación de las topologías LAN.
- Implementación de la topología WAN.
- Diseño del esquema de direccionamiento lógico (IP Classfull, IP ClassLess, Subnetting, CIDR / VLSM Supernetting).
- Configuración de accesos locales (físicos) y remotos a dispositivos de red.
- Configuración de dispositivos de red LAN, Wireless LAN y WAN (Switch, Access Point, Router).
- Configuración de medidas de seguridad de capa 2 en switches.
- Configuración de PCs en la LAN.
- Configuración de VLANs. Enrutamiento entre VLANs.
- Implementación de enrutamiento dinámico, estático y por defecto en routers.
- Configuración de una VPN corporativa, en un escenario tipo “Site-to-Site and Extranet VPN Business”.
- Configuración de medidas de seguridad de capa 3 en routers (filtros de paquetes con ACL extendidas).
- Identificación y resolución de problemas de networking, en caso de ser necesario.

ESCENARIO DE SIMULACIÓN



El ejercicio se realizará EN BASE A LA TOPOLOGÍA Y DATOS del gráfico anterior.

El alumno se desempeñará como Administrador de las **Sucursales A y B, LAN METROPOLITANA y WAN EMPRESARIAL.**

El Administrador debe organizar la topología de las redes LAN y WAN.

El ejercicio puede desarrollarse en una secuencia distinta a la formulada, pero deberán satisfacerse todos los requerimientos indicados. Programe sus tareas para desarrollarlas semana a semana, desde la Nro 4 hasta la Nro 7. DEBERÁ ESTAR RESUELTO PARA LA CLASE DE LA SEMANA PREVISTA EN EL PROGRAMA DE ACTIVIDADES, A FIN DE SU REVISIÓN Y CONSULTA DE DUDAS.

TAREAS DE CONFIGURACIÓN

1. **Como Administrador de la LAN METROPOLITANA:**
   - 1.1. Implemente la topología de la LAN, en base al escenario dado.
   - 1.2. Considere las siguientes IP reservadas para:
     - 1.2.1. WAN Empresarial: 10.0.0.0
     - 1.2.2. LAN METROPOLITANA: 172.16.0.0
     - 1.2.3. SUCURSALES A y B: 192.168.x.0
   - 1.3. Elabore el diseño lógico (direccionamiento IP) de la LAN METROPOLITANA a partir de la dirección reservada 172.16.0.0, con los requisitos indicados a continuación:
     - 1.3.1. Direccionamiento IP estático, con subredes, según corresponda.
     - 1.3.2. Cada PC pertenecerá a la VLAN correspondiente, asignándosele una IP de la subred que se indica:
       - 1.3.2.1. Para la VLAN 1: subred 1 de la red 172.16.0.0/21
       - 1.3.2.2. Para la VLAN 10: subred 10 de la red 172.16.0.0/21
       - 1.3.2.3. Para la VLAN 20: subred 20 de la red 172.16.0.0/21
       - 1.3.2.4. Para la VLAN 30: subred 30 de la red 172.16.0.0/21
       - 1.3.2.5. La PC respectiva deberá tener en el campo de host el número equivalente al Nro de PC. Ejemplo: para la **PC11**, su IP será: A.B.C.**11**.
       - 1.3.2.6. Las PCs cuyos usuarios utilicen información crítica, deberán tener asignadas direcciones IP pares o impares, para facilitar la configuración de filtros de paquetes con ACLs. Los usuarios con menos privilegios, tendrán IP impares o pares, según la política definida.
     - 1.3.3. Para cada subred, la puerta de enlace (Default Gateway) deberá ser la **dirección de host útil anterior** a la IP de broadcast de la subred. Ejemplo: si el valor del último octeto de la IP de broadcast es: **.191**, entonces la IP del Default Gateway será: **.190**.
   - 1.4. Organice la secuencia de configuración, capa por capa de la arquitectura de red LAN: desde ACCESO, pasando por DISTRIBUCIÓN y, luego, NÚCLEO. *Utilice, como herramienta de apoyo, un diagrama de GANTT para registrar la estructura de desglose del trabajo y el estado de avance de cada actividad y/o tarea.*
   - 1.5. Defina medidas adecuadas para asegurar la disponibilidad de los enlaces e implemente la configuración de los switches de distribución y acceso, con el

protocolo STP, para resolver problemas de loops de capa 2 en caso de ser necesario:

1.5.1. Identificación del switch RAÍZ y la configuración de puertos RAÍZ que correspondan.

1.5.2. Configuración de STP en el switch correspondiente, para que sea seleccionado como raíz.

1.5.3. Configuración de agregado de enlace LACP entre los switches de acceso y el de distribución, con el fin de duplicar el ancho de banda, evitando que *spanning tree* bloquee uno de ellos.

1.6. Implemente las VLANs para cumplir los siguientes requisitos de enlace y segmentación de dominios:

1.6.1. VLAN **1**: todos los puertos que no sean asignados a las VLANs de negocio. **Deberá configurarse el enrutamiento de paquetes (tramas) de la VLAN 1 con las otras LANs de las Sucursales A y B, pero no con las VLANs de la LAN METROPOLITANA.**

1.6.2. VLAN **10** GERENCIA: actualmente, 5 gerentes. Se configurará sólo la **PC11. Deberá configurarse el enrutamiento de paquetes (tramas) de la VLAN 10 con las otras LANs de las Sucursales A y B, pero no con las VLANs de la LAN METROPOLITANA.**

1.6.3. VLAN **20** VENTAS: actualmente, 50 vendedores. Se configurarán sólo las **PC24 y PC26**. No deberá permitirse el enrutamiento de paquetes (tramas) de la VLAN 20 con las otras VLANs o LANs.

1.6.4. VLAN **30** LOGISTICA: actualmente, 50 empleados. Se configurarán sólo las **PC35 y PC37**. No deberá permitirse el enrutamiento de paquetes (tramas) de la VLAN 30 con las otras VLANs o LANs.

1.6.5. **NO SE PERMITE EL TRÁFICO ENTRE PC DE DISTINTAS VLANs.**

1.7. Aplique las siguientes medidas de seguridad de dispositivos:

1.7.1. Contraseñas de modo privilegiado en todos los dispositivos: **redes**.

1.7.2. Acceso remoto para administración a todos los dispositivos: sólo permitido para **NO más de 2 accesos simultáneos**, con cierre de sesión automática **después de 2 minutos de inactividad**, con contraseña: **utn**.

1.7.3. **Se requiere seguridad de puerto para todas las PC conectadas**.

1.8. Configure los parámetros de configuración global y la interfaz LAN del router NÚCLEO.

1.9. Configure una ruta estática que permita a cualquier host del segmento **VLAN 10**, alcanzar el DB Server de la Sucursal B.

1.10. Realice todas las pruebas de verificación y validación de comunicaciones en base a los requerimientos.

2. Como Administrador de la Sucursal A:

2.1. Implemente la topología de la LAN, en base al escenario dado, configurando los dispositivos de red y PCs de los segmentos LAN 2 y 3 de esta Sucursal.

2.2. Configure todas las interfaces LAN de los routers NÚCLEO 2 y 3.

2.3. Realice todas las pruebas de verificación y validación de comunicaciones entre todos los dispositivos LAN y puertas de enlace.

2.4. Mediante la Notebook **Admin Sucursal A** configure el dispositivo Linksys Acceso Wireless **p/CLIENTES, en Modo Infraestructura como AP Router, entre los segmentos 3 (192.168.3.0/24 - WLAN Clientes) y 4 (LAN**

192.168.4.0/24), considerando los siguientes datos, políticas y medidas de seguridad:

2.4.1. Parámetros de Administración del AP:
- 2.4.1.1. IP de administración: **192.168.3.1**.
- 2.4.1.2. Contraseña de administración: **redes**.
- 2.4.1.3. Desactivación de administración wireless, de modo remoto y UPnP.

2.4.2. Parámetros básicos de comunicaciones wireless:
- 2.4.2.1. Modo de red: **mixto**.
- 2.4.2.2. SSID: **WLAN_SUC-B**.
- 2.4.2.3. Canal wireless: **4**.
- 2.4.2.4. Desactivación de la difusión del SSID.

2.4.3. Servicios:
- 2.4.3.1. Sólo activar DHCP para hasta 10 dispositivos móviles: de **192.168.3.100** a **192.168.3.109**.

2.4.4. Filtros de direcciones MAC: sólo permitir la **PC3** y la PDA-PT **Cliente MÓVIL.**

2.4.5. Parámetros de cifrado:
- 2.4.5.1. Autenticación: **WPA2-PSK** con clave **redsegura**.
- 2.4.5.2. Encripción o cifrado: **AES**.
- 2.4.5.3. Otros parámetros de comunicaciones y seguridad: **serán definidos por el Administrador de la Sucursal A**, según las "**mejores prácticas**".

2.5. Configure el dispositivo móvil PDA-PT **Cliente MÓVIL** con los datos necesarios para el acceso wireless LAN en el Segmento 3.

2.6. Interconecte correctamente el dispositivo Linksys con el **Switch3**.

2.7. Verifique la comunicación desde la PDA, por lo menos, hasta el **Router3**.

2.8. Aplique todas las medidas de seguridad de dispositivos, indicadas en el apartado **1.7.**

2.9. Asegure el acceso remoto para la administración del dispositivo, desde la **LAN METROPOLITANA**.

3. Como Administrador de la Sucursal B:

3.1. Configure todos los dispositivos involucrados con las medidas de seguridad requeridas.

3.2. Active los servicios web con el protocolo HTTPS en el servidor **DB Server**.

3.3. Realice todas las pruebas de verificación y validación en el entorno LAN.

3.4. Configure la contraseña secreta "redes" como administrador del Router1

3.5. Asegure el acceso remoto para la administración del dispositivo, desde la **LAN METROPOLITANA**. Configure la contraseña de acceso remoto "redes" en la línea virtual 0, sin habilitar otros enlaces virtuales.

3.6. Configure una ruta por defecto desde el Router1 hacia el router NUCLEO de la LAN METROPOLITANA. **Para observar el funcionamiento del tráfico por el túnel IPSec, agregue una ruta estática hacia la red 192.168.3.0 mediante el router NÚCLEO.**

3.7. Mediante la Laptop “Adm Sucursal B” configure en el Router1 **un acceso VPN desde la Sucursal B**, considerando los siguientes datos, políticas y medidas de seguridad:

3.7.1. Configure el método de intercambio de claves “Internet Key Exchange” con los siguientes datos:
- 3.7.1.1. ID de política: **1**.
- 3.7.1.2. Método de autenticación mediante *clave simétrica*.
- 3.7.1.3. Algoritmo Hash: **SHA**.
- 3.7.1.4. Algoritmo de Cifrado: **AES**, con longitud de clave **256**.
- 3.7.1.5. Protocolo de establecimiento de sesión con *clave simétrica*: **Diffie-Hellman con clave de 1536 bits.**
- 3.7.1.6. Tiempo máximo de vida: **4 minutos**.

3.7.2. Establezca la clave simétrica con el extremo B del Túnel, en la interfaz WAN del **Ruter3** (IP: **10.0.3.2**), configurando el valor: **redes**.

3.7.3. Configure del direccionamiento IPSec en modo túnel, asignando al túnel el ID **50** y los algoritmos de autenticación y cifrado: **ah-sha-hmac esp-3des**.

3.7.4. Configure un filtro de paquetes en el extremo B del túnel, mediante una lista de control de acceso extendida con el ID **102**, que permita como destino del túnel a la red **192.168.3.0**, solamente para todos los paquetes originados en cualquier host de la red de la Sucursal B, IP: **192.168.1.0**.

3.7.5. Configure el mapa que determina la IP del extremo remoto (B) del túnel y el tráfico de interés que será encapsulado con los parámetros de funcionamiento y seguridad:
- 3.7.5.1. Nombre del mapa: **mapa-ab**
- 3.7.5.2. Tiempo de vida: **900** segundos.
- 3.7.5.3. Filtro de paquetes: **102**.

3.7.6. Configure el Router3 con los parámetros necesarios del extremo A del Túnel IPSec. **Para observar el funcionamiento del tráfico por el túnel IPSec, agregue una ruta estática hacia la red 192.168.1.0 mediante el router NÚCLEO.**

3.7.7. Active el túnel IPSec sobre la interfaz serie correspondiente del Router1.

3.7.8. Mediante la Notebook **Admin Sucursal B** configure el dispositivo Linksys Acceso Wireless **p/CLIENTES, en Modo Infraestructura como Bridge, entre los segmentos WLAN (VENTAS) y LAN, en la red 192.168.1.0/24**, considerando los siguientes datos, políticas y medidas de seguridad:

3.7.9. Parámetros de Administración del AP:
- 3.7.9.1. IP de administración: **192.168.1.10**.
- 3.7.9.2. Contraseña de administración: **redes**.
- 3.7.9.3. Desactivación de administración wireless, de modo remoto y UPnP.

3.7.10. Parámetros básicos de comunicaciones wireless:
- 3.7.10.1. Modo de red: **mixto**.
- 3.7.10.2. SSID: **WLAN_SUC-A**.
- 3.7.10.3. Canal wireless: **9**.
- 3.7.10.4. Desactivación de la difusión del SSID.

3.7.11. Servicios:
3.7.11.1. Sólo activar DHCP para hasta 5 dispositivos móviles: de **192.168.1.100** a **192.168.1.104**.
3.7.12. Filtros de direcciones MAC: sólo permitir la PDA-PT **VENDEDOR 1**.
3.7.13. Parámetros de cifrado:
3.7.13.1. Autenticación: **WPA2-PSK** con clave **redsegura**.
3.7.13.2. Encripción o cifrado: **AES**.
3.7.13.3. Otros parámetros de comunicaciones y seguridad: **serán definidos por el Administrador de la Sucursal B**, según las "**mejores prácticas**".

3.8. Configure el dispositivo móvil Laptop-PT **VENDEDOR 1** con los datos necesarios para el acceso wireless LAN en el Segmento 1.
3.9. Interconecte correctamente el dispositivo Linksys con el **Switch1**.
3.10. Verifique la comunicación desde la PDA, por lo menos, hasta el **Router1**.
3.11. Aplique todas las medidas de seguridad de dispositivos, indicadas en el apartado **1.7.**

4. **Como Administrador de la WAN EMPRESARIAL:**

4.1. Realice la configuración de todos los dispositivos en el entorno WAN, considerando los siguientes requerimientos:
4.1.1. Se utilizará el protocolo de enrutamiento **RIP versión 2 ó EIGRP para el sistema autónomo 1**.
4.1.2. El Direccionamiento IP, se diseñará en base a la información inserta en el gráfico. La Dir IP de la interfaz WAN deberá ser la Dir IP más baja de las direcciones útiles de la red respectiva.
4.1.3. Verifique el funcionamiento correcto del enrutamiento dinámico y estático.

5. Como CISO (Chief Information Security Officer) de la WAN EMPRESARIAL:
5.1. Diseñe e implemento filtros ACLs que:
5.1.1. Desde la LAN METROPOLITANA sólo puedan acceder al DB Server de las SUCURSAL B con servicio HTTPS habilitado, las PCs de la VLAN 30.
5.1.2. Desde la LAN METROPOLITANA sólo pueda acceder remotamente a todos los routers de la WAN, la PC 1 de la VLAN 1 (instalarla y conectarla dónde corresponda, física y lógicamente).
5.1.3. Desde la LAN METROPOLITANA sólo pueda probar la comunicación con todos los routers de la WAN, mediante la aplicación PING desde la PC 1 de la VLAN 1.
5.2. Pruebe su funcionamiento con el resto del Sistema Empresarial.

6. RESULTADOS ESPERADOS:

6.1. Demuestre que puede acceder desde la **PC3** al sitio Web corporativo, activo en el equipo **DB Server**.

6.2. Demuestre el acceso Web desde la PDA al equipo **DB Server**, activo en la Sucursal B.

6.3. Realice un *traceroute* desde cualquiera de los hosts del Segmento 3 de la Sucursal A y verifique el túnel IPSec configurado.

6.4. Pruebe el funcionamiento correcto de:

6.4.1. Cableado LAN y WAN. (**topología correcta y sincronismo WAN**)

6.4.2. Segmentación de VLANs Gerencia, Ventas y Logística. (**Ping correcto dentro de la VLAN – Ping fallido fuera de la VLAN**)

6.4.3. Direccionamiento de las redes y subredes IP. (**Pings entre segmentos de distintas LANs**)

6.4.4. Enrutamiento dinámico con entradas del protocolo respectivo. (**Tabla de enrutamiento con las entradas R o E correspondientes**)

6.4.5. Comunicación de LAN METROPOLITANA a otras LANs remotas (**Ping y Traceroute correctos**)

6.4.6. Comunicación de los dispositivos móviles hasta los respectivos Gateway de las Sucursales A y B.

6.4.7. La seguridad de capa 2 (de puerto LAN) que correspondan a las PCs de la LAN METROPOLITANA.

6.4.8. Las medidas de seguridad para la administración de todos los dispositivos.

6.4.9. Funcionamiento correcto de la comunicación dentro del segmento IPv6, y de éste con los restantes IPv4.

6.4.10. Funcionamiento de los filtros ACLs, para cada caso requerido (***se debe probar al final, para verificar el resto de los procesos de comunicaciones***).