REDES 2

Proyecto de Fin de Curso

Escenario Integrador
Diseño de esquema de direccionamiento, simulación y configuración de una red corporativa y pruebas de conectividad.

2025-1

Trabajo Grupal: Escenario Integrador

1 Objetivo de aprendizaje

- Diseñar el esquema de direccionamiento para la topología proporcionada.
- Implementar la topología en un simulador de red.
- Realizar las configuraciones necesarias para el funcionamiento de la red.
- Evidenciar el correcto funcionamiento a través de pruebas de comunicación.

2 Insumo

Materiales de clase (PPTs, PDFs, Escenarios de laboratorios, Grabaciones, etc)
Software de simulación Cisco Packet Tracer

3 Plazos

Presentación de informe: Semana 15
Exposición Grupal: Semana 16

4 Contexto

En esta tarea, se les proporciona una dirección de red inicial para diseñar un esquema de direccionamiento VLSM. Sobre la base de un conjunto de requisitos, asignarán subredes y direccionamiento.

Como parte de esta tarea, deberán implementar una red en el software de simulación Cisco Packet Tracer. Primero, deben realizar la conexión de los dispositivos de red de acuerdo con la topología que se muestra más adelante y posteriormente deberán configurarlos de modo que admitan conectividad IPv4. A continuación, configurarán VLANs, RoAS, DHCPv4, OSPFv2, GRE, NAT, y STP en la red. Finalmente, deberán verificar la conectividad.

Para el diseño del esquema de direccionamiento cada grupo tendrá su propia dirección de base de acuerdo con la siguiente estructura:
10.X.Y.0/255.255.255.0

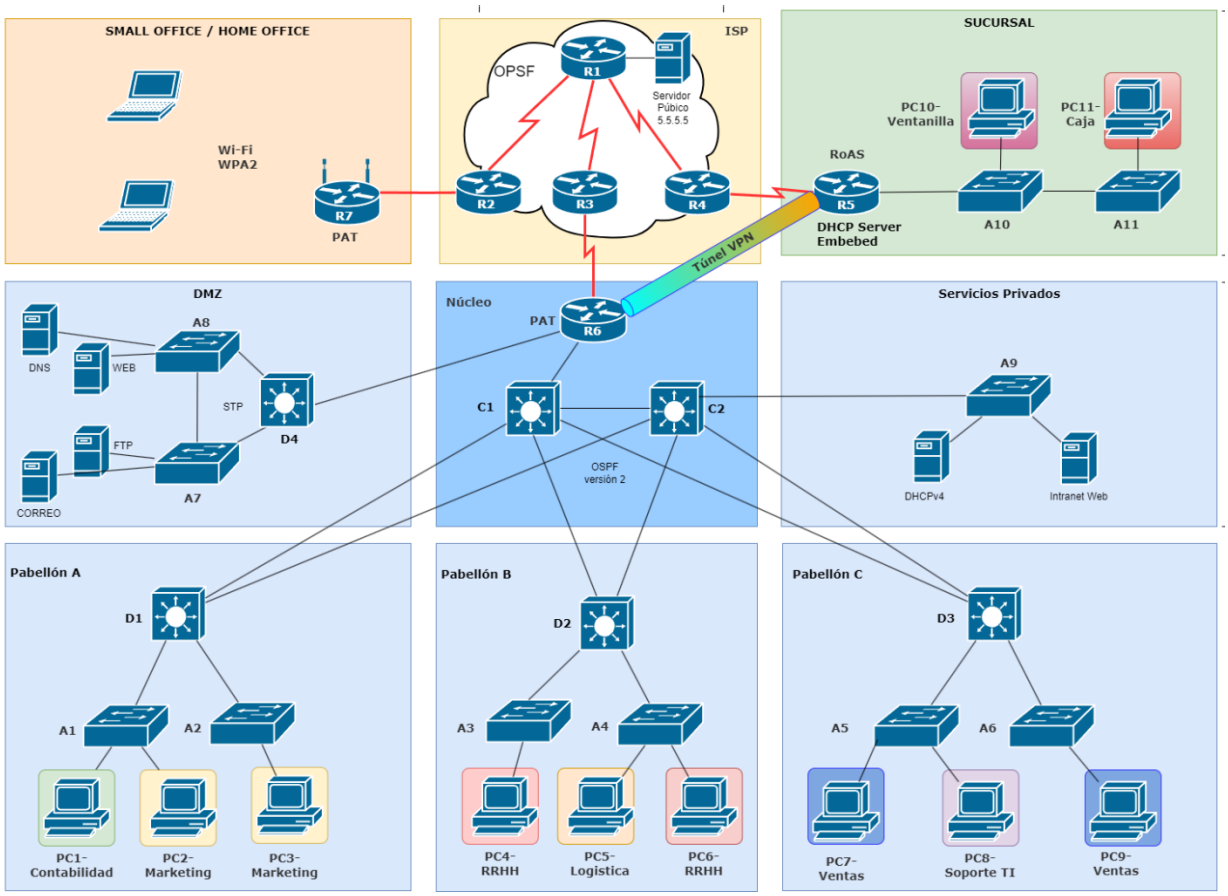
Donde:

X: Número de grupo (por ejemplo, para NRC 10380 => X = 80)
Y: Número de grupo (por ejemplo, para Grupo 3 => Y = 3)

Algunos ejemplos:

Para el Grupo 1, y NRC 10380; la dirección base sería: 10.80.1.0/255.255.255.0
Para el Grupo 3, y NRC 10380; la dirección base sería: 10.80.3.0/255.255.255.0
Para el Grupo 5, y NRC 10381; la dirección base sería: 10.81.5.0/255.255.255.0

A continuación, se muestra el diagrama topológico que deberán implementar en el software de simulación.



Dispositivos intermedios sugeridos:

- Switch Capa 2: Modelo 2960
- Switch Capa 3: Modelo 3650
- Routers (1-6): Modelo 4321 (Agregar uno o dos módulos MIN-2T para conectar cables seriales)
- Router 7 (SOHO): WRT300N o HomeRouter

Descripción de la topología:

La topología está segmentada en colores diferentes, lo que indica diferentes zonas o sucursales de una organización.

Zona Superior Izquierda (Color Beige – Small Office / Home Office):

- Dos computadoras portátiles conectadas a una red Wi-Fi protegida con WPA2.
- Se utiliza PAT (Port Address Translation) para traducir una dirección IP pública entre las computadoras.
- Configurar el router inalámbrico con IP pública, máscara y puerta de enlace para que pueda tener acceso a internet. La dirección IP pública para este dispositivo la encontrara en la Tabla de Subnetting WAN en las siguientes páginas.

Zona Superior Central (Color Amarillo Claro – Proveedor de Servicios de Internet – ISP):

- Hay un servidor público con la dirección IP: 5.5.5.5.
- Todos los routers tienen asignadas direcciones IP públicas (ver tabla de subnetting WAN).
- Implemente las interconexiones entre routers (R1-R2, R1-R3, R1-R4, R3-R6 y R4-R5) utilizando puertos y cables seriales.
- La Interconexión entre R7 y R2, se realiza con cable de cobre mediante interfaces ethernet.
- El enrutamiento interno en la red del ISP (Routers R1, R2, R3, y R4), se implementa mediante el protocolo OSPF versión 2.

Zona Superior Derecha (Color Verde - Sucursal):

- Muestra dos VLANs, una nombrada como "Ventanilla" (PC10) y otra como "Caja" (PC11).
- El router R5 debe enrutar las VLAN utilizando Routing On a Stick (RoAS), y también funciona como un servidor DHCP embebido para las redes de PC10 y PC11.
- El router R5 tiene un túnel VPN con el protocolo GRE hacia el Router R6 y una Ruta Estática Predeterminada para acceder a la WAN (ISP) y enrutamiento estático para enrutar el tráfico a través de la VPN.
- El router R5 traduce las direcciones Privadas hacia internet utilizando NAT sobre cargado (PAT).

Zona Central izquierda (Color Azul - DMZ):

- En la DMZ, hay servidores DNS, WEB, FTP, y Correo. Todos ellos están conectados a unos switches que implementan STP (Spanning Tree Protocol). El Switch D4 debe ser configurado como Root Primary y el Switch A8 como Root Secondary.
- La red de servidores de la DMZ utiliza el pool de IPs públicas: 100.225.48.0/27. (Ver Tabla de direccionamiento DMZ).
- El Switch D4 solo funciona como Switch Layer 2, y la puerta de enlace de la DMZ se configura en R6

Zona Central (Color Azul - Núcleo):

- El núcleo de la red tiene un router, y dos switches multicapa. Se utiliza OSPF (Open Shortest Path First) para el enrutamiento interno y una ruta estática predeterminada recursiva para encaminar el tráfico hacia la WAN (ISP).
- El router de borde (R6) es el encargado de las traducciones para las redes privadas del campus y realiza la traducción utilizando NAT sobre cargado (PAT).
- El router R6 tiene un túnel VPN con el protocolo GRE hacia el Router R5. Y enrutamiento estático para enrutar el tráfico a través de la VPN.

Zona Central Derecha (Color Azul - Servicios Privados):

- Hay dos (2) servidores conectados a un switch, etiquetados como "Intranet Web" y "DHCPv4". Se debe considerar una VLAN adicional para la red de Servidores Privados

Zona Inferior (Color Azul - Pabellón A y B):

- Cada pabellón tiene varios PCs asignados a diferentes departamentos como Contabilidad, Marketing, Logística, Recursos Humanos, Ventas y Soporte de TI. (cada departamento se implementa en una VLAN independiente)
- Hay un switch central en cada pabellón. D1 para el Pabellón A, D2 para el Pabellón B, y D3 para el Pabellón C.
- El enrutamiento entre VLANs se implementa dentro de los switches multicapa (D1, D2 y D3), utilizando interfaces virtuales de switch (SVIs).
- El enrutamiento entre la capa de distribución (Switches D1, D2, y D3) y la capa de Núcleo (Switches C1, y C2) se implementa mediante el protocolo OSPF versión 2.

La topología presentada es una combinación de redes LAN y WAN con varios protocolos de enrutamiento y segmentación de red para control de acceso y optimización del tráfico. Se utilizan tecnologías como VPN para la conectividad segura entre diferentes ubicaciones y OSPF para el enrutamiento dinámico. La presencia de una DMZ indica que se ofrecen servicios a usuarios externos mientras se protege la red interna. Las VLANs se utilizan para la segmentación lógica de la red dentro de los pabellones.

5 Indicaciones

Estructura del informe:

- Caratula (Nombre del curso, NRC, número de grupo, integrantes del grupo)
- Índice
- Resumen Ejecutivo (Breve descripción del proyecto, objetivos y conclusiones)
- Introducción
  - Importancia del diseño de redes
  - Importancia de la simulación de las redes
  - Objetivos de la tarea académica
- Diseño del esquema de direccionamiento
- Implementación en el Simulador
- Configuración de la Red
- Pruebas y Validación
- Conclusiones
- Recomendaciones
- Bibliografía
- Anexos
  - Cualquier otra información adicional que respalde el trabajo (códigos de configuración, scripts, etc.).

Para realizar el laboratorio ten en cuenta lo siguiente:

Diseño de esquema de direccionamiento:

Requerimientos
Calcule las subredes para las siguientes subredes

- Contabilidad: 16 host
- Marketing: 10 host
- Logística: 5 host
- Recursos humanos: 5 host
- Ventas: 4 host

- Soporte TI: 2 host
- Servidores Privados: 5 host
- Sucursal Ventanilla: 4 host
- Sucursal Caja: 4 host
- Small Office Home Office: 6 host

Para los enlaces entre Routers y Switches Multicapa calcule 8 subredes a partir de la dirección 172.20.16.128/25

1. Enlace entre D1 y C1: 2 host
2. Enlace entre D1 y C2: 2 host
3. Enlace entre D2 y C1: 2 host
4. Enlace entre D2 y C2: 2 host
5. Enlace entre D3 y C1: 2 host
6. Enlace entre D3 y C2: 2 host
7. Enlace entre C1 y C2: 2 host
8. Enlace entre C1 y R6: 2 host

Para el direccionamiento de la red del Proveedor de Servicios de Internet considerar la siguiente tabla de subnetting.

Tabla de Subnetting WAN

Descripción	Dirección	Mascara	Primera IP	Ultima IP
R1->R2	80.8.1.0	255.255.255.252	80.8.1.1	80.8.1.2
R1->R3	80.8.1.4	255.255.255.252	80.8.1.5	80.8.1.6
R1->R4	80.8.1.8	255.255.255.252	80.8.1.9	80.8.1.10
R2->R7	80.8.1.12	255.255.255.252	80.8.1.13	80.8.1.15
R3->R6	80.8.1.16	255.255.255.252	80.8.1.17	80.8.1.18
R4->R5	80.8.1.20	255.255.255.252	80.8.1.21	80.8.1.22
R1->Server	5.5.5.0	255.255.255.0	5.5.5.1	5.5.5.254

Para el subnetting de las redes LAN debe completar la tabla de subnetting correspondiente de manera similar a la tabla de subnetting WAN.

Tabla de Subnetting LAN

Descripción	Dirección	Mascara	Primera IP	Ultima IP

Y adicionalmente deberá elaborar la tabla de direccionamiento (Puede utilizar una hoja de cálculo) con la siguiente estructura:

Tabla de Direccionamiento General

Equipo*	Interfaz	Dirección IP	Mascara	Default Gateway**

(*) Considere computadoras, Servidores, routers y switches multicapa (excluya la DMZ).
(**) Tome en cuenta que los routers no requieren la configuración de una puerta de enlace predeterminada.

Para la red DMZ se trabajará con el pool de direcciones publicas: **200.20.20.0/28.** De acuerdo son la siguiente tabla de direccionamiento:

Tabla de Direccionamiento DMZ

Equipo*	Interfaz	Dirección IP	Mascara	Default Gateway**
Web	NIC	100.225.48.2	255.255.255.224	100.225.48.1
DNS	NIC	100.225.48.3	255.255.255.224	100.225.48.1
Correo	NIC	100.225.48.4	255.255.255.224	100.225.48.1
FTP	NIC	100.225.48.5	255.255.255.224	100.225.48.1

Tabla de VLANs:

Complete la siguiente tabla de VLANs seleccionando los ID y nombres de acuerdo a su criterio.

Área *	VLAN ID	VLAN Name
Contabilidad		
Marketing		
Logística		
Recursos Humanos		
Soporte TI		
Servidores Privados		
Ventas		
Caja		

(*) Para otras áreas que no se encuentren especificadas en la presenta tabla puede utilizar la VLAN 1. Y para la configuración de la VLAN Nativa puede usar el ID 99.

Simulación:

Pabellones A B y C

- Cree las VLANs
- Configure los puertos de acceso
- Configure los puertos troncales
- Configure la VLAN Nativa
- Configure el enrutamiento intervlan con los switches multicapa
- Los hosts deben funcionar como clientes DHCPv4.
- Habilite el reenvío DHCPv4 para alcanzar al servidor DHCP ubicado en la red de servicios privados.

Servicios Privados

- Personalice la página web del servidor Intranet Web y asegúrese que solo este habilitado el servicio HTTPs por cuestiones de seguridad.

- Configure el servidor DHCPv4 para que reparta direcciones a los clientes de las VLANs de los pabellones A, B y C.

Zona desmilitarizada (DMZ)

- Personalice la página web
- Configure 4 usuarios en el servidor FTP
- Configure 13 cuentas de correo* en el servidor de correo utilizando el dominio @upn.edu.pe
- Configure registros de tipo A para los siguientes nombres de dominio
    - www.upn.pe
    - ftp.upn.pe
    - ns.upn.pe
    - mail.upn.pe

(*) Configure los clientes de correo en las VLANs de los pabellones A, B y C, en la Sucursal y otro en la Red SOHO.

- Configure STP en los switches y asegure que el switch D4 sea el puente raíz principal, y que el switch A8 sea el puente raíz secundario. Además, habilite la opción portfast y la protección BPDU en los puertos de acceso hacia los servidores.

Zona Núcleo

- Configure el protocolo OSPF de área única para enrutar el tráfico entre todas las redes dentro del Campus. Tenga en cuenta que también será necesario habilitar OSPF en los Switches multicapa D1, D2, y D3 (Utilice la opción no switchport para habilitar los puestos enrutados en los switches multicapa D1, D2, D3, C1, y C2)
- Configure una ruta predeterminada en R6 para enviar el tráfico hacia internet
- Habilite el reenvío de la ruta predeterminada a través del protocolo OSPF.
- Configure NAT Sobrecargado (overload) para traducir las direcciones privadas con la IP pública de la interfaz serial de R6.
- Configure el túnel VPN utilizando el protocolo GRE.

Zona Small Office Home Office

- Utilice un router inalámbrico con interfaz gráfica de configuración (GUI).
- Dependiendo del equipo seleccionado complete a su criterio los siguientes parámetros a utilizar para la configuración

Parámetros	Valores
SSID	
Banda	
Número de Canal	
Modo de Seguridad	
Encriptación	
Contraseña	

- Personalice la configuración de la interfaz LAN y habilitar el servicio DHCP mediante la interfaz gráfica de configuración de su router, personalice las direcciones IP de la red LAN de acuerdo con la Subred asignada (Ver Tabla de Subnetting LAN).
- Personalizar la configuración de la interfaz Internet.

Zona Sucursal

- Cree las VLANs (Revise su tabla de VLANs)

- Configure puertos de acceso y puertos troncales
- Personalice la VLAN nativa con el ID 99.
- Configure el Enrutamiento intervlan en R5 utilizando Router on a Stick.
- Configure una Ruta predeterminada en R5 para dar acceso a internet
- Configure NAT sobrecargado para traducir las direcciones privadas con la IP publica de la interfaz WAN de R5.
- Configure el servicio DHCPv4 embebido en R5 (para el DNS utilice la IP pública del servidor ubicado en la DMZ)
- Configure un cliente de correo en la PC Ventanilla.
- Complete la configuración del Túnel VPN hacia R6 utilizando el protocolo GRE.

Zona ISP

- Configure el enrutamiento interno utilizando OSPF de área única.
- Configure el servidor Público, como un servidor web con la IP 5.5.5.5/24.
- Agregue una ruta estática recursiva en R3 hacia la red pública DMZ 100.225.48.0/27.
- Redistribuya la ruta estática en R3 hacia los otros routers utilizando el comando “redistribute static subnets” dentro del modo de configuración de OSPF “(config-router)#

6 Evaluación y puntaje

Para la evaluación de esta tarea académica se aplicará la siguiente rubrica analítica. Tome en cuenta los siguientes criterios a la hora de desarrollar su trabajo.

Indicadores	NIVEL			Puntaje
	Muy bien	**En proceso**	**No cumple**	
Presentación y Estructura del Informe (15%) -Documentación-	El informe está perfectamente organizado, incluye todas las secciones requeridas y sigue una lógica clara. La portada, el índice y los anexos están completos y bien presentados.	El informe tiene una estructura básica, pero le faltan algunas secciones o tiene una organización deficiente. La portada, el índice o los anexos están incompletos.	El informe carece de estructura, la portada, el índice y los anexos son inadecuados o están ausentes.	
	3 puntos	2 puntos	1 puntos	
Diseño de Topología y Esquema de Direccionamiento (20%) -Documentación-	Diseño de topología excepcionalmente detallado y completo, con un esquema de direccionamiento lógico y bien fundamentado.	Diseño de topología básico y esquema de direccionamiento funcional, pero con varias áreas que requieren mejora.	Diseño de topología y esquema de direccionamiento incompletos o incorrectos.	
	4 puntos	2 punto	1 puntos	
Configuración en el Simulador (30%) -Archivo PKT-	Implementación impecable en el simulador, con todas las configuraciones correctas y bien documentadas	Implementación parcial con errores en las configuraciones que afectan la funcionalidad de la red.	Implementación pobre o incorrecta con documentación deficiente.	
	6 puntos	3 puntos	1 puntos	
Pruebas y Validación (20 %) -Exposición-	Pruebas exhaustivas y bien documentadas que demuestran claramente el funcionamiento de la red.	Pruebas básicas realizadas, con documentación insuficiente o resultados que dejan dudas sobre la funcionalidad.	Pruebas insuficientes, mal documentadas o que no demuestran la funcionalidad de la red	
	4 puntos	2 punto	1 puntos	
Conclusiones (15 %) -Exposición-	Análisis crítico detallado con conclusiones que reflejan una comprensión profunda del proyecto	Análisis adecuado con conclusiones coherentes, pero que podrían beneficiarse de mayor profundidad o detalle	Análisis y conclusiones deficientes o ausentes	
	3 puntos	2 punto	1 puntos	

Instrucciones para la entrega

- El documento en formato PDF y el archivo de simulación en formato PKT se entregará a través del campus virtual.
- Colocar los datos completos de todos los integrantes que participaron en el desarrollo del proyecto.