Facultad de Ingenierías y Tecnología de la Información y Comunicación

Escuela de Tecnología Información para la Gestión de los Negocios

Escuela de Ingenierías de Sistemas Informáticos

Diseño e Implementación de una Infraestructura de Red Segmentada mediante VLANs con Integración de Servicios de Red y Aplicación de Mecanismos Básicos de Ciberseguridad en un Entorno Multidepartamental para la empresa NexaCapital S.A.

BTI-13 Redes 2

Profesor:

Daniel Adolfo Ramírez González

Unidad Responsable:

D.A.S Solutions

Elaborado Por:

David Abarca Chaves (202001610152)

Alberto Álvarez Navarro (20210110651)

Sebastián Chaves Solano (20200120941)

Santiago Ramírez Elizondo (202401112941)

San José, 15 de mayo del 2025

1. **Introduccion:**

La empresa NexaCapital es un organismo reconocido por sus servicios de préstamos y por su manejo y enseñanzas de finanzas en relación a inversión a largo y corto plazo, está creciendo actualmente en la industria, y recientemente ha ampliado la cantidad de empleados y departamentos dentro de ella por la alta demanda que están presentando con la inestabilidad del dólar. El servicio de red interno de la empresa nunca ha sido su fuerte, esto debido a que se manejaban con un sistema básico y poco complicado porque no tenían capital para manejar lo que esto conlleva.

Como ya han logrado establecer un nombre y una reputación positiva ante el público, han ganado más experiencia y compromiso, por lo que tienen que buscar cómo mejorar la conexión, seguridad y escalabilidad de red para una comunicación interna más fuerte y un proceso mejor estructurado. Actualmente, la empresa ha agregado 3 departamentos más, siendo un total de 4 departamentos. Entre ellos están: Finanzas, Tecnología de la Información (TI), Administración y Recursos Humanos.

La situación actual presenta varios problemas, en los que se ve comprometida la información y los datos de los empleados y clientes, junto con la seguridad de red y de la comunicación interna. Ante esta problemática, han decidido estructurar su programa de redes a algo más escalable, automatizado y sólido. Para esto, se quiere aplicar servicios básicos de ciberseguridad como Listas de Control de Accesos (ACLs), un sistema con VLANs e implementar servicios como DNS, DHCP, correo y net corporativas.

Objetivo General:

- Solucionar las necesidades y dificultades de la empresa “NexaCapital” con el proceso de crecimiento empresarial y la implementación de un sistema de redes robusto y seguro.

Objetivos Específicos:

- Maximizar los procesos de automatización en la red debido a un incremento de personal en la empresa.
- Implementar servicios de seguridad para la red y así asegurar un flujo continuo en el envío de datos sensibles.
- Lograr la estandarización de los mejores protocolos en el servicio de red de la empresa.

Marco Teórico

1. Modelos de Referencia en Redes: OSI y TCP/IP

El modelo OSI (Open Systems Interconnection) es un marco conceptual que estandariza las funciones de un sistema de comunicación en siete capas: física, enlace de datos, red, transporte, sesión, presentación y aplicación (Tanenbaum & Wetherall, 2011). Este modelo facilita el diseño y la interoperabilidad de sistemas heterogéneos.

Por otro lado, el modelo TCP/IP es el conjunto de protocolos fundamentales para Internet y redes empresariales, compuesto por cuatro capas: enlace, internet, transporte y aplicación (Kurose & Ross, 2021). TCP/IP es más pragmático y ampliamente utilizado en entornos reales, siendo la base para el direccionamiento IP y protocolos como TCP, UDP, DNS y DHCP.

Estos modelos guían el diseño e implementación de redes escalables y seguras, como el que se plantea para NexaCapital, facilitando la segmentación lógica y el control del tráfico.

2. Switching y Enrutamiento

El **switching** o conmutación de paquetes se encarga de la transferencia de datos dentro de una misma red local (LAN), trabajando principalmente en la capa 2 del modelo OSI (enlace de datos). Los switches permiten segmentar la red en dominios de colisión reducidos, mejorando el rendimiento (Stallings, 2017).

El **enrutamiento** funciona en la capa 3 (red), facilitando la comunicación entre diferentes redes o subredes. Los routers analizan las direcciones IP de los paquetes y determinan la mejor ruta para su envío. En NexaCapital, el enrutamiento interno eficiente garantiza que el tráfico entre VLANs y departamentos se dirija correctamente.

3. VLANs (Redes de Área Local Virtuales)

Las VLANs permiten segmentar una red física en múltiples redes lógicas, facilitando la organización y seguridad del tráfico de datos (Cisco Systems, 2020). Gracias a IEEE 802.1Q, el etiquetado de tramas permite que múltiples VLANs coexistan en un mismo enlace físico, asegurando aislamiento y control.

En NexaCapital, la implementación de VLANs para cada departamento (Finanzas, TI, Recursos Humanos, etc.) mejora la seguridad y optimiza el uso del ancho de banda.

4. Servicios de Red: DNS, DHCP y Correo Electrónico

- **DNS (Domain Name System)** traduce nombres de dominio amigables a direcciones IP, permitiendo una navegación y comunicación sencilla dentro de la red (Mockapetris, 1987).

- **DHCP (Dynamic Host Configuration Protocol)** automatiza la asignación de direcciones IP y parámetros de red, facilitando la administración y escalabilidad (Droms, 1997).

- **Correo electrónico corporativo** es fundamental para la comunicación interna y externa; sistemas como Exchange o Zimbra proporcionan plataformas robustas con integración, seguridad y gestión de usuarios.

Estos servicios automatizan y mejoran la eficiencia de la red interna de NexaCapital, permitiendo un manejo profesional de recursos.

5. Seguridad en Redes: ACLs

Las **Listas de Control de Acceso (ACLs)** son reglas que controlan el tráfico entrante y saliente en dispositivos de red, filtrando paquetes según direcciones IP, puertos y protocolos, mejorando la seguridad y evitando accesos no autorizados (Odom, 2020). En NexaCapital todo esto garantizará un entorno seguro para la transmisión de datos sensibles, protegiendo la confidencialidad e integridad de la información.

6. Arquitectura de Red Jerárquica

El diseño jerárquico de redes divide la infraestructura en capas funcionales: acceso, distribución y núcleo (Cisco Systems, 2018). Este modelo mejora la escalabilidad, administración y resiliencia de la red.

- **Capa de acceso:** conecta dispositivos finales (PCs, impresoras).

- **Capa de distribución:** agrega tráfico y aplica políticas.

- **Capa núcleo:** ruta de alta velocidad entre distribuidores.

Este enfoque permite a NexaCapital crecer sin comprometer el rendimiento ni la seguridad.

7. Normativas y Estándares Aplicables

La **Ley 8968** de Protección de Datos en Costa Rica exige salvaguardar la confidencialidad, integridad y disponibilidad de los datos personales, requisito fundamental para el manejo seguro en redes (Paniagua & Alvarado, 2019).

El cumplimiento de estándares internacionales como **ISO 27001** y **NIST** garantiza la implementación de buenas prácticas en seguridad informática y gestión de riesgos (ISO, 2013; NIST, 2018).

8. **Factibilidad Técnica:**

   A. **Soluciones Tecnológicas Evaluadas:**

Solución	**Características**	**Ventajas**	**Desventajas**
Red tradicional con VLANs, ACLs, servidores locales	Infraestructura física centralizada con servicios DNS, DHCP, correo y red corporativa en servidores propios. Segmentación por VLANs y control mediante ACLs.	Mayor control interno, personalización total, sin dependencia de terceros.	Mayor inversión inicial en hardware, requiere mantenimiento técnico continuo.
Infraestructura híbrida (local + servicios en la nube)	Parte de los servicios (como correo y almacenamiento) en la nube, como Microsoft 365 o Google Workspace. DNS/DHCP internos. Red física con VLANs.	Reducción en mantenimiento, alta disponibilidad, acceso remoto sencillo.	Dependencia de conectividad externa, posibles costos recurrentes en suscripciones.

Selección Final:

Se opta por infraestructura local con potencial a híbrida, dado que la empresa desea controlar sus servicios internos, pero está abierta a escalar hacia la nube en el futuro.

   A. **Requerimientos técnicos:**

      a. **Análisis de acuerdo a la arquitectura de red:**

Departamentos	Total de trabajadores (Conexion alámbrica Obligatoria)	Dispositivos con conexión Inalámbrica (cel, laptop, tablet,	Total Final
Finanzas	50	60	110
RRHH	20	24	44
TI	14	17	31
Administración	10	12	22
Total de dispositivos:	**94**	**113**	**207**

Departamentos	Total Final	Routers C.Dist	Cantidad switches (24 puertos)	# Switch por departamento
Finanzas	50	A	2.08	2 (A y B)
RRHH	20	A	0.83	1 (C)
Administración	10	B	0.42	1 (D)
TI	14	B	0.58	1 (D)
Totales	196	2	3.92	
Total final de switches a utilizar			4	

El primer cuadro estima la demanda por departamento: cuántos usuarios requieren conexión alámbrica y cuántos dispositivos se conectarán por Wi-Fi, sumando 207 endpoints en total (94 cableados y 113 inalámbricos). Con base en esa carga, el segundo cuadro dimensiona el acceso: al dividir los requerimientos cableados entre 24 puertos se obtiene el número de switches necesarios (Finanzas ≈2.08→2, RRHH ≈0.83→1, Administración ≈0.42→1, TI ≈0.58→1), para ~4 switches en total. También se muestra a qué router de distribución (A–D) se conectará cada switch y, en Finanzas, se reparten 2 switches entre A y B para redundancia.

b. Hardware:

Se concluye con un resumen técnico necesario mínimo con las siguientes características:

Componente	Modelo	Unidades
Routers Core	Cisco ISR 4321	1
Routers Distribución	Cisco ISR 4321	2
Switches de Acceso	Cisco Catalyst 2960X-48TS-LL	4
Puntos de Acceso WiFi	Cisco Catalyst 9120AX-B (Wi-Fi 6)	4
Servidores físicos	Dell PowerEdge R650	1
UPS empresariales	APC SMT1500RM2UC	2

C. Software :

- IOS XE / NX-OS (enrutadores y switches)
- Cisco DNA Center (opcional para control centralizado)

- pfSense o Fortinet Firewall virtualizado (si no se usa hardware dedicado)
- DNS/DHCP: Bind9 / Windows Server 2022
- Correo corporativo: Exchange, Zimbra, o integración con GSuite / O365
- Antivirus centralizado y sistema de inventario TI

D. Conectividad:

- Backbone a 10 Gbps entre switches core y de acceso (SFP+)
- Red interna con Gigabit Ethernet
- PoE para puntos de acceso
- Internet empresarial simétrico (mínimo 500 Mbps, preferible 1 Gbps)

E. Estándares:

- IEEE 802.3bz (2.5/5/10GBASE-T)
- IEEE 802.1Q (VLAN tagging)
- IEEE 802.11ax (WiFi 6)
- IEEE 802.3af/at/bt (PoE)
- ISO 27001 y NIST para políticas de seguridad
- TIA-568 para cableado estructurado

Compatibilidad con Sistemas Existentes:

Actualmente, NexaCapital opera con un sistema básico sin segmentación de red ni servidores dedicados. Sin embargo:

- Las estaciones de trabajo existentes son compatibles con redes Ethernet y pueden conectarse a VLANs.
- No existen dependencias intrínsecas de sistemas heredados de alta complejidad, lo cual facilita la migración a la nueva infraestructura de red segmentada.
- Se utilizarán componentes de hardware ya existentes siempre que cumplan con los nuevos estándares (por ejemplo, switches no gestionables se reemplazan, pero PCs, impresoras u otros dispositivos compatibles se conservan).

Escalabilidad y sostenibilidad tecnológica:

La solución propuesta es altamente escalable y está pensada para acompañar en cada proceso del crecimiento de la empresa a corto, mediano y largo plazo:

- La red se estructura modularmente por VLANs, lo que facilita la integración de nuevos departamentos.
- El direccionamiento IP se planifica con subredes expansibles, permitiendo agregar dispositivos sin rediseño total.
- Los servidores tienen capacidad de virtualización, lo que permite instalar nuevos servicios sin comprar nuevo hardware físico.

- El diseño contempla la posibilidad de migrar servicios (como correo o almacenamiento) a la nube en el futuro sin afectar la operación actual.
- Se definen políticas de mantenimiento preventivo y actualizaciones, promoviendo la sostenibilidad operativa.

9. Factibilidad Económica y Financiera:

- **Costo estimado del proyecto:**

Componente	Modelo	Unidades	Precio por	Total	Fuente
Dispositivos principales					
Routers Core	Cisco ISR 4321	1	$ 627.00	$ 627.00	itprice
Routers Distribución	Cisco ISR 4331	2	$ 1,066.00	$ 2,132.00	itprice
Switches de Acceso	Cisco Catalyst 2960X	4	$ 1,040.00	$ 4,160.00	itprice
Puntos de Acceso WiFi	Cisco Catalyst 9120AX-B (Wi-Fi 6)	4	$ 811.00	$ 3,244.00	itprice
Servidores físicos	Dell PowerEdge R650	1	$ 6,769.00	$ 6,769.00	eBay
UPS empresariales	APC SMT1500RM2UC	1	$ 2,259.99	$ 2,259.99	CDW
Cableado Estructurado					
Cables	UTP CAT6 gris	2200	$ 0.50	$ 1,100.00	Ferretería Venecia
Gabinete o Racks	De piso 42U	1	$ 423.67	$ 423.67	Amazon
Canaletas	Curvas, uniones, cajas de salida, tapas y anclajes incluidos	300	$ 6.28	$ 1,884.00	CQ NET
Patch Panel	CAT6 de 48 puertos	3	$ 73.90	$ 221.70	Amazon
Conectores	Macho, hembra y para PP	113	$ 3.02	$ 341.26	eBay
Servicios Profesionales					
Mano de obra especializada		1	$ 7,500.00	$ 7,500.00	D.A.S Solutions
Documentación técnica, pruebas y mantenimiento		1	$ 1,500.00	$ 1,500.00	D.A.S Solutions
Presupuesto final total:				$ 32,162.62	₡ 16,081,310.00

- **Fuentes de financiamiento:**

La empresa podría financiar este proyecto mediante una combinación de:

A. Capital propio (reinversión de utilidades debido al crecimiento reciente).
B. Créditos empresariales o leasing tecnológico, con entidades financieras nacionales (ej. Banco Nacional, BCR, BAC).
C. Fondos de inversión para transformación digital, como incentivos públicos o privados en sectores financieros.
D. Alianzas estratégicas con integradores tecnológicos (como D.A.S Solutions) que permitan modelos de financiamiento escalonado o servicios gestionados.

- **Proyecciones de costos de operación y mantenimiento:**

Concepto	Estimado anual (USD)	Observaciones
Mantenimiento de hardware	$2 000 – $3 000	Limpieza, revisión de cableado, UPS, APs
Licencias y actualizaciones	$1 000 – $2 000	Equipos Cisco (opcional según modelo)
Soporte técnico externo (outsourcing)	$3 000 – $5 000	Soporte correctivo y monitoreo proactivo
Consumo eléctrico estimado	$1 000 – $1 500	UPS, switches, servidores (24/7)
Reemplazo de componentes menores	$500 – $1 000	Patch cords, conectores, fuentes de poder

Total aproximado anual: $7 500 – $12 500

- **Retorno o beneficios esperados:**
  A. **Económicos:**
    i. Reducción de pérdidas por fallos de red y tiempos muertos.
    ii. Aumento de productividad interna (conectividad, colaboración).
    iii. Mejor aprovechamiento de sistemas de información y bases de datos.
    iv. Reducción de costos de soporte externo no planificado.
    v. Escalabilidad sin necesidad de rediseños costosos en el corto plazo.

  B. Sociales:
    i. Mejora en la comunicación interdepartamental, especialmente en atención al cliente.
    ii. Ambiente laboral más eficiente y tecnológico.
    iii. Facilita el teletrabajo parcial o trabajo remoto seguro.

  C. Ambientales:
    i. Uso eficiente de energía mediante switches PoE, UPS inteligentes y menos cantidad de hardware (por consolidación)
    ii. Menor necesidad de traslados físicos o impresiones, promoviendo procesos digitales.
    iii. Posibilidad de implementar sistemas de monitoreo ambiental o energético internos a futuro.

Cronograma de Implementación:

Fase	Actividad	Duración (días)	Responsables
0. Inicio	Kickoff, alcance, plan de trabajo	1	Líder de proyecto (PM), patrocinador
1. Relevamiento	Site survey, inventario, mapas de puertos	1	Ing. de redes, técnico de cableado
2. Diseño lógico	VLANs, direccionamiento, OSPF, BGP, plan DNS/DHCP, correo	2	Arquitecto de red, D.A.S Solutions
3. Diseño físico	Topología, ubicación de equipos, energía/rack, patch panels	1	Arquitecto de red, infra TI, D.A.S Solutions
4. Procura	Compra y licencias de routers, switches, APs, S.O. servidores	3	Compras, proveedor, PM
5. Preconfiguración	Plantillas, hardening básico y backups iniciales	2	Ing. de redes
6. Laboratorio	Pruebas de OSPF/BGP, DHCP/DNS, correo, ACLs	2	Ing. de redes, D.A.S Solutions
7. Cableado	Tendido, canalizaciones, certificación y etiquetado	2	Técnicos de cableado
8. Instalación	Montaje de routers/switches/APs en sitio	1	Ing. de redes, técnicos
9. Acceso (Switches)	VLANs, trunks, VTP (si aplica), Port-Security, deshabilitar puertos	1	Ing. de redes
10. Core/Enrutamiento	Enlaces /30, OSPF interno, BGP con ISP, rutas por defecto	1	Ing. de redes, ISP (Liberty)
11. Servicios	DHCP scopes, zonas DNS, intranet HTTP, SMTP/IMAP/POP3	2	D.A.S Solutions
12. Validación	Pruebas end-to-end (intra/inter-VLAN), correo, Wi-Fi, rendimiento	2	QA, Ing. redes, usuarios clave
13. Piloto	Migración del depto. TI y corrección de hallazgos	1	PM, Ing. redes, Mesa de ayuda
14. Despliegue total	Migración por ventanas a Finanzas, RRHH y Admin	1	PM, Ing. redes, D.A.S Solutions
15. Hypercare	Monitoreo intensivo, KPIs, afinamientos	3	NOC/Soporte, D.A.S Solutions
Total del tiempo:		26 días (3-4 semanas)	

10. Riesgos Generales:

a. Riesgos Identificados

- **Técnicos:** Fallas en la configuración de servicios de red o conflictos IP
- **Operativo:** Resistencia al cambio o falta de capacitación en el nuevo sistema.
- **Financieros:** Aumento de costos por adquisición de equipos o servicios
- **Legales:** Incumplimiento en protección de datos personales

b. Terceros Afectados

Los terceros afectados por la implementación del nuevo sistema de red en NexaCapital incluyen tanto factores internos como externos.

En primer lugar, los clientes se verán beneficiados de forma indirecta, ya que sus datos estarán más protegidos y el servicio será más ágil y confiable. Por otro lado, los funcionarios internos experimentan un impacto directo, ya que deberán adaptarse a nuevas tecnologías y procedimientos, lo que implica capacitación y cambios en su rutina laboral.

También se verán involucrados los proveedores tecnológicos, quienes podrán participar en la venta, instalación o soporte de equipos y servicios relacionados con la red. Finalmente, instituciones gubernamentales y entidades regulatorias podrían verse afectadas positivamente, al verificar que NexaCapital cumple con las normativas vigentes sobre seguridad y tratamiento de datos.

c. Plan de Mitigación de Riesgos

Tipo de Riesgo	Descripción del Riesgo	Impacto	Plan de Mitigación
Técnico	Fallas en la configuración de servicios de red (DNS, DHCP, VLANs)	Alta	Realizar pruebas en un entorno controlado (Packet Tracer o laboratorio) antes de la implementación final. Documentar toda configuración.
Operativo	Resistencia del personal al cambio tecnológico	Media	Implementar un plan de capacitación gradual y acompañamiento en la transición. Crear manuales y soporte técnico.
Financiero	Aumento de costos por equipos no presupuestados o mantenimiento	Alta	Establecer margen de contingencia en el presupuesto y realizar cotizaciones previas.
Legal	Incumplimiento de normativas de protección de datos	Alta	Asesoría legal previa a la implementación. Cumplir Ley 8968 y realizar auditorías internas periódicas.
Seguridad	Accesos no autorizados o mal uso de la red	Alta	Aplicar ACLs, políticas de contraseñas seguras, firewall y control de acceso físico a los equipos.

Desarrollo:

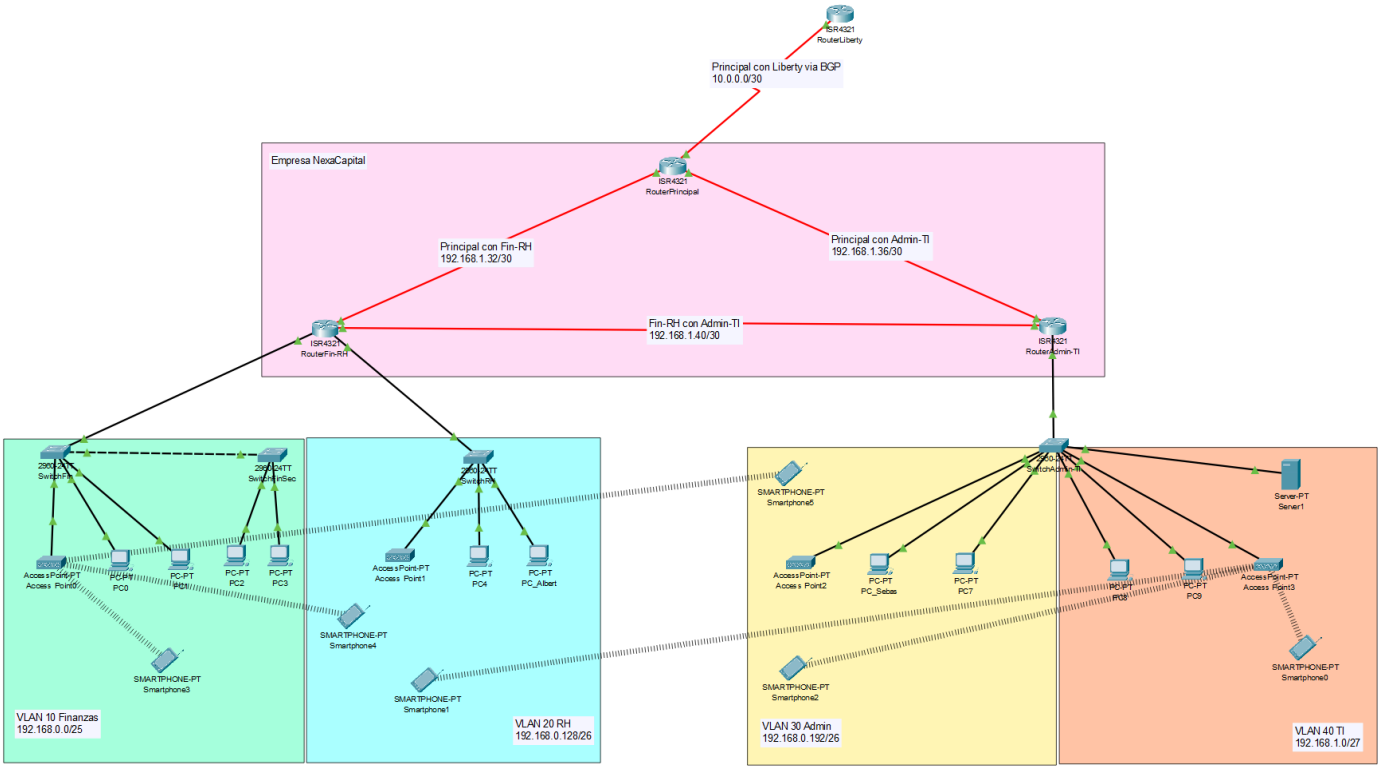
Subneteo, direccionamiento IP y orden de Red:

Se aplicó VLSM partiendo de la red principal 192.168.0.0/24 Max 254 host: a Finanzas (110 hosts) se le asigna 192.168.0.0/25 (255.255.255.128) con rango .0–.127 y gateway .1; a RRHH (44 hosts) 192.168.0.128/26 (.128–.191, gateway .129); a TI (31 hosts) 192.168.0.192/26 (.192–.255, gateway .193). Como el /24 queda completo, Administración (22 hosts) se ubica en el siguiente bloque como 192.168.1.0/27 (255.255.255.224, gateway 192.168.1.1). Los enlaces punto a punto entre routers usan /30 para optimizar direcciones: 192.168.1.32/30, 192.168.1.36/30 y 192.168.1.40/30; y la salida al ISP emplea 10.0.0.0/30 para BGP. Se usan los wildcards respectivos para OSPF/ACLs y se reserva siempre la primera IP como gateway y la última como broadcast.

Dept.	Hosts Req. (Permitidos)	Máscara de Subred/bits	Wilcard	Red	Primera / Gateway	Última	Broadcast
Finanzas	110 (126)	255.255.255.128	0.0.0.127	192.168.0.0	192.168.0.1	192.168.0.126	192.168.0.127
RRHH	44 (62)	255.255.255.192	0.0.0.63	192.168.0.128	192.168.0.129	192.168.0.190	192.168.0.191
TI	31 (62)	255.255.255.192	0.0.0.63	192.168.0.192	192.168.0.193	192.168.0.254	192.168.0.255
Administración	22 (30)	255.255.255.224	0.0.0.31	192.168.1.0	192.168.1.1	192.168.1.30	192.168.1.31
Principal con Fin-RH	2 (2)	255.255.255.252	0.0.0.3	192.168.1.32	192.168.1.33	192.168.1.34	192.168.1.35
Principal con Admin-TI	2 (2)	255.255.255.252	0.0.0.3	192.168.1.36	192.168.1.37	192.168.1.38	192.168.1.39
Fin-RH con Admin-TI	2 (2)	255.255.255.252	0.0.0.3	192.168.1.40	192.168.1.41	192.168.1.42	192.168.1.43
Principal con Liberty via BGP	2 (2)	255.255.255.252	0.0.0.3	10.0.0.0	10.0.0.1	10.0.0.2	10.0.0.3

Sistema de red jerárquico para NexaCapital:

El sistema adopta una topología jerárquica: un Router Principal en el core, dos routers de distribución (Fin-RRHH a la izquierda y Admin-TI a la derecha) y la capa de acceso con switches y APs. La red está segmentada por VLAN: VLAN10 Finanzas 192.168.0.0/25, VLAN20 RRHH 192.168.0.128/26, VLAN30 Administración 192.168.0.192/26 y VLAN40 TI 192.168.1.0/27; cada VLAN sale por su gateway (.1) en subinterfaces y los switches truncan hacia los routers para el enrutamiento inter-VLAN. Entre los tres routers se usan enlaces /30 (1.32/30, 1.36/30 y 1.40/30) corriendo OSPF para anunciar todas las redes internas y lograr redundancia. El Router Principal se conecta al ISP por 10.0.0.0/30 con BGP, redistribuyendo la ruta por defecto al resto. Los APs extienden la conectividad inalámbrica por VLAN y en TI reside el servidor (DNS/HTTP/Correo) accesible desde todos los departamentos. A continuación, se presenta una captura de su respectiva implementación/simulación en Cisco Packet Tracer:



Códigos de configuración:

A continuación, se brinda una pequeña explicación de los comandos y configuraciones por dispositivos.

- **Routers de distribución (RouterFin-RH y RouterAdmin-TI):**

Estos equipos realizan el enrutamiento inter-VLAN ("router-on-a-stick"). Para ello crean subinterfaces en los puertos Gigabit y etiquetan tráfico con **encapsulation dot1Q** para las VLAN 10 (Finanzas), 20 (RRHH), 30 (Administración) y 40 (TI), asignando en cada una la **ip address** que actúa como gateway (.1, .129, .193 y 1.1, respectivamente). Los enlaces WAN entre routers usan interfaces Serial con /30 y **bandwidth 1544** (simulación de E1/T1). El enrutamiento interno se habilita con OSPF (**router ospf 1** y sentencias **network … area 0** para anunciar subredes y enlaces). Además, cada VLAN tiene su pool DHCP con **ip dhcp pool**, **network**, **default-router** y **dns-server 192.168.1.2**, automatizando la entrega de IPs. Comandos como **no ip domain-lookup** y **description** mejoran operatividad y documentación.

- **Router principal e ISP (Liberty):**

El RouterPrincipal se enlaza al ISP mediante la red **10.0.0.0/30** en **Serial0/1/0**. Con el ISP se establece **BGP** (**router bgp**, **neighbor … remote-as**) y se habilita la redistribución de rutas entre

protocolos: el principal **redistribuye OSPF hacia BGP** y, a la inversa, **BGP hacia OSPF** para que las redes internas aprendan la ruta de salida y el ISP vea los prefijos corporativos. También anuncia por OSPF los enlaces /30 internos y define **router-id 1.1.1.1** para estabilidad del proceso.

- **Switches de acceso:**

Se crean las **VLANs** (10, 20, 30, 40) y se asignan **puertos de usuario en modo access** (**switchport mode access**, **switchport access vlan …**). Los enlaces ascendentes hacia los routers y entre switches operan como **trunks** con **switchport mode trunk** y **switchport trunk allowed vlan …**; **nonegotiate** evita DTP. En TI se activa **STP PortFast** y **BPDU Guard** para proteger puertos de borde. El hardening básico incluye **enable secret**, contraseñas en **consola** y **VTY**, y **logging synchronous** para sesiones más claras.

- **Servicios (DNS, correo e intranet):**

El servidor interno (192.168.1.2) ofrece **DNS** con registros **A** y **CNAME** para el dominio (p. ej., *www.nexacapital.com* y *nexacapital.com*), y entradas de **correo** (*mail.nexacapital.com*). El **Mail Server** habilita **SMTP** y **POP3** con el dominio indicado, y el **HTTP Server** publica las páginas de intranet. Los routers apuntan a este DNS desde DHCP con **dns-server 192.168.1.2**, integrando resolución de nombres y entrega de IPs.

A continuación, se presentan todos los comandos y código referente con las configuraciones de routers, switches, protocolos y servicios del sistema de red implementado en Cisco Packet Tracer.

Routers:

```
###################### Router Liberty ##############################

ena

conf t

hostname RouterLiberty

no ip domain-lookup


interface Serial0/1/0

description Conexión a RouterPrincipal

ip address 10.0.0.2 255.255.255.252

bandwidth 1544

no shutdown
```

```
exit

! BGP
router bgp 100
neighbor 10.0.0.1 remote-as 200
exit


######################## Router Principal ################################
ena
conf t
hostname RouterPrincipal
no ip domain-lookup

! Interfaces
interface Serial0/1/0
description Conexión a RouterLiberty
ip address 10.0.0.1 255.255.255.252
bandwidth 1544
no shutdown
exit

interface Serial0/1/1
description Conexión a RouterFin-RH
ip address 192.168.1.33 255.255.255.252
bandwidth 1544
no shutdown
```

```
exit

interface Serial0/2/0
description Conexión a RouterAdmin-TI
ip address 192.168.1.37 255.255.255.252
bandwidth 1544
no shutdown
exit

! OSPF (anuncio de enlaces internos/seriales)
router ospf 1
router-id 1.1.1.1
network 192.168.1.32 0.0.0.3 area 0
network 192.168.1.36 0.0.0.3 area 0
redistribute bgp 200 subnets
exit

! BGP (conexión a Liberty y anuncio de OSPF hacia BGP)
router bgp 200
neighbor 10.0.0.2 remote-as 100
redistribute ospf 1
exit
############### RouterFin-RH ###################################
ena
conf t
hostname RouterFin-RH
no ip domain-lookup
```

```
interface Serial0/1/1
description Conexión a RouterPrincipal
ip address 192.168.1.34 255.255.255.252
bandwidth 1544
no shutdown
exit

interface Serial0/2/1
description Conexión a RouterAdmin-TI
ip address 192.168.1.41 255.255.255.252
bandwidth 1544
no shutdown
exit

! OSPF
router ospf 1
network 192.168.0.0 0.0.0.127 area 0
network 192.168.0.128 0.0.0.63 area 0
network 192.168.1.32 0.0.0.3 area 0
network 192.168.1.40 0.0.0.3 area 0
exit

interface GigabitEthernet0/0/0
description Hacia SwitchFin (trunk VLAN 10)
no shutdown
exit
```

```
interface GigabitEthernet0/0/1
description Hacia SwitchRH (trunk VLAN 20)
no shutdown
exit

! Subif VLAN 10 (Finanzas) 192.168.0.0/25  Gateway .1
interface GigabitEthernet0/0/0.10
encapsulation dot1Q 10
description VLAN10-Finanzas
ip address 192.168.0.1 255.255.255.128
exit

! Subif VLAN 20 (RRHH) 192.168.0.128/26  Gateway .129
interface GigabitEthernet0/0/1.20
encapsulation dot1Q 20
description VLAN20-RRHH
ip address 192.168.0.129 255.255.255.192
exit

ip dhcp pool VLAN10_FIN
network 192.168.0.0 255.255.255.128
default-router 192.168.0.1
dns-server 192.168.1.2
domain-name nexacapital.com
```

```
ip dhcp pool VLAN20_RH
network 192.168.0.128 255.255.255.192
default-router 192.168.0.129
dns-server 192.168.1.2
domain-name nexacapital.com

################ RouterAdmin-TI ####################################
ena
conf t
hostname RouterAdmin-TI
no ip domain-lookup

interface Serial0/2/0
description Conexión a RouterPrincipal
ip address 192.168.1.38 255.255.255.252
bandwidth 1544
no shutdown
exit

interface Serial0/2/1
description Conexión a RouterFin-RH
ip address 192.168.1.42 255.255.255.252
bandwidth 1544
no shutdown
exit

! OSPF
```

```
router ospf 1
network 192.168.0.192 0.0.0.63 area 0
network 192.168.1.0 0.0.0.31 area 0
network 192.168.1.36 0.0.0.3 area 0
network 192.168.1.40 0.0.0.3 area 0
exit

interface GigabitEthernet0/0/0
description Hacia SwitchAdmin-TI (trunk 30,40)
no shutdown
exit

interface GigabitEthernet0/0/0.30
encapsulation dot1Q 30
description VLAN30-Admin
ip address 192.168.0.193 255.255.255.192
exit

interface GigabitEthernet0/0/0.40
encapsulation dot1Q 40
description VLAN40-TI
ip address 192.168.1.1 255.255.255.224
exit

ip dhcp pool VLAN30_ADMIN
network 192.168.0.192 255.255.255.192
default-router 192.168.0.193
```

dns-server 192.168.1.2

domain-name nexacapital.com

ip dhcp pool VLAN40_TI

network 192.168.1.0 255.255.255.224

default-router 192.168.1.1

dns-server 192.168.1.2

domain-name nexacapital.com

Switches:

################## SwitcheFin ##########################

ena

conf t

hostname SwitchFin

no ip domain-lookup

vlan 10

name FINANZAS

exit

! Puertos de usuario a VLAN 10

interface range fa0/1-24

switchport mode access

switchport access vlan 10

exit

```
! Uplink al router (si aplica) por G0/1 en VLAN 10
interface g0/1
description Uplink a Router Fin-RH
switchport mode trunk
switchport trunk allowed vlan 10
switchport nonegotiate
exit

! Enlace a SwitchFinSec (trunk solo VLAN 10)
interface g0/2
description Trunk a SwitchFinSec g0/1
switchport mode trunk
switchport trunk allowed vlan 10
switchport nonegotiate
exit



end
wr

! seguridad switches
ena
conf t

! ===== Clave para modo privilegiado =====
enable secret N3x@2025
```

```
! ===== Console =====
line console 0
 password N3x@2025
 login
 logging synchronous
exit

! ===== VTY (0 a 4) =====
line vty 0 4
password N3x@2025
login
logging synchronous
exit

end
wr

################## SwitcheFinSec ############################
ena
conf t
hostname SwitchFinSec
no ip domain-lookup

vlan 10
name FINANZAS
exit
```

```
! Puertos de usuario a VLAN 10
interface range fa0/1-24
switchport mode access
switchport access vlan 10
exit

! Enlace desde este switch a SwitchFin (trunk)
interface g0/1
description Trunk a SwitchFin g0/2
switchport mode trunk
switchport trunk allowed vlan 10
switchport nonegotiate
exit



end
wr

! seguridad switches
ena
conf t

! ===== Clave para modo privilegiado =====
enable secret N3x@2025

! ===== Console =====
line console 0
```

```
 password N3x@2025
 login
 logging synchronous
exit

! ===== VTY (0 a 4) =====
line vty 0 4
password N3x@2025
login
logging synchronous
exit

end
wr

################### SwitcheRH ############################
ena
conf t
hostname SwitchRH
no ip domain-lookup

vlan 20
 name RH
exit

! Puertos de usuario a VLAN 20
interface range fa0/1-24
```

```
switchport mode access
switchport access vlan 20
exit

! Uplink al router en VLAN 20 (si aplica)
interface g0/1
description Uplink a Router Fin-RH (VLAN 20)
switchport mode trunk
switchport trunk allowed vlan 20
switchport nonegotiate
exit



end
wr

! seguridad switches
ena
conf t

! ===== Clave para modo privilegiado =====
enable secret N3x@2025

! ===== Console =====
line console 0
 password N3x@2025
 login
```

```
 logging synchronous
exit

! ===== VTY (0 a 4) =====
line vty 0 4
password N3x@2025
login
logging synchronous
exit

end
wr

################## SwitcheAdmin-TI ############################
ena
conf t
hostname SwitchAdmin-TI
no ip domain-lookup

vlan 30
name ADMIN
vlan 40
name TI
exit

! Fa0/1 - Fa0/12 en VLAN 30
interface range fa0/1-12
```

```
switchport mode access
switchport access vlan 30
exit

! Fa0/13 - Fa0/24 en VLAN 40
interface range fa0/13-24
switchport mode access
switchport access vlan 40
spanning-tree portfast
spanning-tree bpduguard enable
exit

! Uplink al Router Admin-TI por G0/1 como trunk (router-on-a-stick)
interface g0/1
description Trunk a Router Admin-TI
switchport mode trunk
switchport trunk allowed vlan 30,40
switchport nonegotiate
exit


end
wr

! seguridad switches
ena
conf t
```

```
! ===== Clave para modo privilegiado =====
enable secret N3x@2025

! ===== Console =====
line console 0
 password N3x@2025
 login
 logging synchronous
exit

! ===== VTY (0 a 4) =====
line vty 0 4
password N3x@2025
login
logging synchronous
exit

end
wr
```

Servicios:

```
################### DNS Server ####################
IP address: 192.168.1.2
DNS Service: On
Tipo: A record
```

Name: www.nexacapital.com

Address: 192.168.1.2

Tipo: C NAME

Name: nexacapital.com

Host: www.nexacapital.com

Para mail:

Tipo: A record

Name: mail.nexacapital.com

Address: 192.168.1.2

Servidor SMTP: mail.nexacapital.com

Servidor POP3: mail.nexacapital.com

############# Mail Server ######################

SMTP Service: ON

POP3 Service: ON

Domain Name: mail.nexacapital.com

Usuarios: integrantes

passwords: 1234

############# HTTP Server ######################

######################### index.html:

```
<html>
  <head>
    <title>NexaCapital - Finanzas</title>
  </head>
```

```
  <body>
    <center><font size="+2" color="blue">NexaCapital</font></center>
    <hr>
    Bienvenido a <b>NexaCapital</b>, un organismo reconocido por sus
    <b>servicios de préstamos</b> y por la <b>enseñanza de finanzas</b> para
    inversión a corto y largo plazo. Crecemos de la mano de nuestros clientes,
    ofreciendo claridad y acompañamiento en cada decisión.

    <p>
      La reciente volatilidad del dólar incrementó la demanda y nos llevó a
      ampliar nuestro equipo y departamentos para servirte mejor.
    </p>

    <p>Quick Links:
      <br><a href="historia.html">Nuestra historia</a>
      <br><a href="mailto:info@nexacapital.com">Contacto</a>
      <br><a href="logo.jpg">Logo</a>
    </p>
  </body>
</html>
```

########################## historia.html:

```
<html>
  <head>
    <title>NexaCapital - Historia</title>
  </head>
  <body>
```

```
    <center><font size="+2" color="blue">Nuestra historia</font></center>
    <hr>

    <p>
      <b>Origen:</b> NexaCapital nació con la misión de acercar el crédito
      responsable y la educación financiera a personas y negocios, impulsando
      inversiones seguras a <i>corto</i> y <i>largo</i> plazo.
    </p>

    <p>
      <b>Crecimiento:</b> La inestabilidad cambiaria aumentó la demanda de
      asesoría y préstamos. Para responder, la empresa amplió su plantilla y
      reestructuró procesos internos.
    </p>

    <p>
      <b>Hoy contamos con 4 departamentos:</b>
      Finanzas, Tecnología de la Información (TI), Administración y
      Recursos Humanos. Aunque nuestro corazón es <b>finanzas</b>, estamos
      modernizando nuestra comunicación interna y sistemas para atenderte con
      mayor rapidez y transparencia.
    </p>

    <p><a href="index.html">← Volver al inicio</a></p>
  </body>
</html>
```

Seguridad:

############### RouterFin-RH ###########

VLAN 10 - FINANZAS

ena

conf t

!

access-list 110 deny ip 192.168.0.0 0.0.0.127 192.168.0.128 0.0.0.63

access-list 110 deny ip 192.168.0.0 0.0.0.127 192.168.0.192 0.0.0.63

access-list 110 deny ip 192.168.0.0 0.0.0.127 192.168.1.0 0.0.0.31

access-list 110 permit ip any any

!

interface fa0/0.10

ip access-group 110 in

end

exit

VLAN 20 - RH

ena

conf t

!

access-list 120 deny ip 192.168.0.128 0.0.0.63 192.168.0.0 0.0.0.127

access-list 120 deny ip 192.168.0.128 0.0.0.63 192.168.0.192 0.0.0.63

access-list 120 deny ip 192.168.0.128 0.0.0.63 192.168.1.0 0.0.0.31

access-list 120 permit ip any any

!

interface fa0/0.20

ip access-group 120 in

end

######### RouterAdmin-TI #############3

VLAN 30 - ADMIN

ena

conf t

!

access-list 130 deny ip 192.168.0.192 0.0.0.63 192.168.0.0 0.0.0.127

access-list 130 deny ip 192.168.0.192 0.0.0.63 192.168.0.128 0.0.0.63

access-list 130 deny ip 192.168.0.192 0.0.0.63 192.168.1.0 0.0.0.31

access-list 130 permit ip any any

!

interface fa0/0.30

ip access-group 130 in

end

VLAN 40 - TI

ena

conf t

!

access-list 140 deny ip 192.168.1.0 0.0.0.31 192.168.0.0 0.0.0.127

access-list 140 deny ip 192.168.1.0 0.0.0.31 192.168.0.128 0.0.0.63

access-list 140 deny ip 192.168.1.0 0.0.0.31 192.168.0.192 0.0.0.63

access-list 140 permit ip any any

!

interface fa0/0.40

ip access-group 140 in

end

Principales protocolos y servicios utilizados:

- DNS: Se implementaría para que los usuarios no tengan que memorizar las direcciones IP y puedan acceder fácilmente a los servicios internos como el correo o internet.
- DHCP: Este se basa principalmente en la automatización del proceso de asignación de IPs, ya que va a haber un incremento importante en el personal y se necesita un orden estructurado en este proceso.
- VLANs: Se implementarán para segmentar la red en dominios de broadcast más pequeños y seguros, separando el tráfico por departamentos o funciones. Esto mejora el rendimiento, facilita la administración y aumenta la seguridad al aislar el tráfico de diferentes áreas.
- Correos: SMTP y PO3/IMAP: Principalmente, se integrará para establecer comunicación interna entre los diferentes departamentos y eventualmente, también se exterioriza el contacto.
- Intranet corporativa HTTP: Se logrará el acceso a información importante interna, tal como comunicados, manuales o noticias.
- Enrutamiento OSPF: Este enrutamiento es para que el router pueda comunicar todas las VLANs sin tener que agregar rutas manualmente y de esta manera, optimizar el proceso.
- Enrutamiento BGP: Será utilizado para la interconexión con redes externas, como el ISP, garantizando el intercambio de rutas de manera dinámica y eficiente. Esto permitirá escalabilidad, redundancia y una mejor selección de rutas hacia internet u otras sedes.
- Seguridad switches: Se incluyen la configuración de contraseñas seguras en el modo privilegiado, línea de consola y líneas VTY, además de habilitar el cifrado de contraseñas y deshabilitar puertos no utilizados.
- Otros tentativos (ciberseguridad):
    - ACLs (Listas de Control de Acceso): Bloquearía el acceso innecesario entre VLANs, dejando que pase solo el tráfico necesario y deseado.

Resultados:

A. Pruebas realizadas:

1. Switches (Layer 2):

1.1. show vlan brief → Puertos de usuario en la VLAN correcta (10/20/30/40).

Switch Fin:

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active
10   FINANZAS                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Switch RH:

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Gig0/2
20   RH                                active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Switch: Admin-TI:

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Gig0/2
30   ADMIN                             active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
40   TI                                active    Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

1.2. show interfaces trunk → Trunks UP y con Allowed VLANs: 10,20,30,40.

Switch Fin:

```
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      on           802.1q         trunking      1
Gig0/2      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Gig0/1      10
Gig0/2      10

Port        Vlans allowed and active in management domain
Gig0/1      10
Gig0/2      10

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      10
Gig0/2      10
```

Switch RH:

```
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Gig0/1      20

Port        Vlans allowed and active in management domain
Gig0/1      20

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      20
```

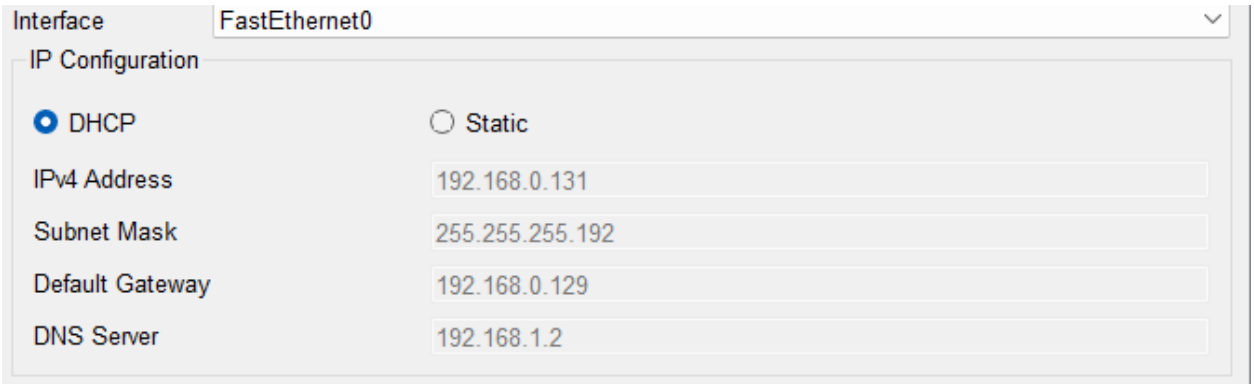
Switch: Admin-TI:

```
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Gig0/1      30,40

Port        Vlans allowed and active in management domain
Gig0/1      30,40

Port        Vlans in spanning tree forwarding state and not pruned
Gig0/1      30,40
```

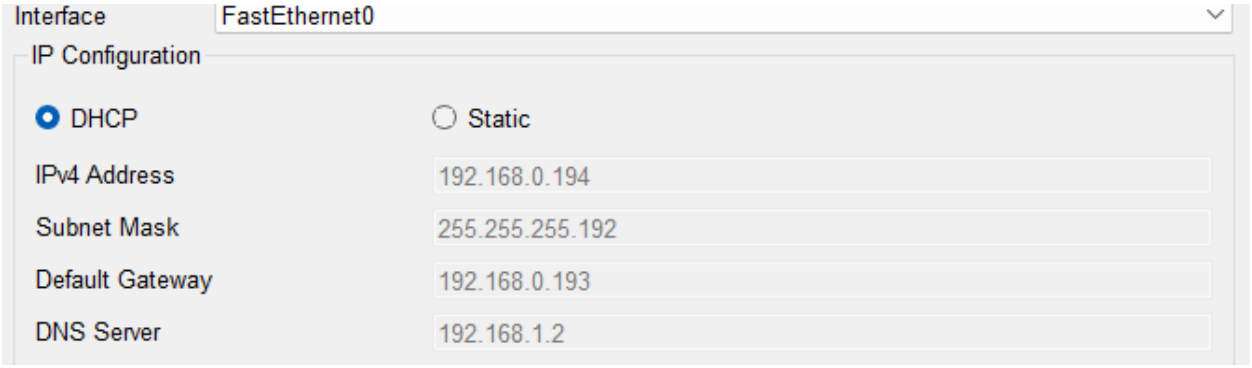
2. En algunas PC's:

2.1. ipconfig /all → IP/máscara/gateway/DNS de su VLAN.

PC Alberto en RH:



PC Sebas en Admin:



3. OSPF:

3.1. show ip ospf neighbor → vecinos Full con los otros routers.

Router Fin-RH:

```
Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1           0   FULL/  -        00:00:38    192.168.1.33    Serial0/1/1
192.168.1.42      0   FULL/  -        00:00:39    192.168.1.42    Serial0/2/1
```

Router Admin-TI:

```
Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1           0   FULL/  -        00:00:34    192.168.1.37    Serial0/2/0
192.168.1.41      0   FULL/  -        00:00:34    192.168.1.41    Serial0/2/1
```

Router Principal:

```
Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.1.41      0   FULL/  -        00:00:34    192.168.1.34    Serial0/1/1
192.168.1.42      0   FULL/  -        00:00:34    192.168.1.38    Serial0/2/0
```

3.2. show ip route → presencia de rutas de todas las subredes internas.

Router Fin-RH:

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.0.0/24 is variably subnetted, 5 subnets, 3 masks
C       192.168.0.0/25 is directly connected, GigabitEthernet0/0/0.10
L       192.168.0.1/32 is directly connected, GigabitEthernet0/0/0.10
C       192.168.0.128/26 is directly connected, GigabitEthernet0/0/1.20
L       192.168.0.129/32 is directly connected, GigabitEthernet0/0/1.20
O       192.168.0.192/26 [110/65] via 192.168.1.42, 02:14:22, Serial0/2/1
     192.168.1.0/24 is variably subnetted, 6 subnets, 3 masks
O       192.168.1.0/27 [110/65] via 192.168.1.42, 02:14:22, Serial0/2/1
C       192.168.1.32/30 is directly connected, Serial0/1/1
L       192.168.1.34/32 is directly connected, Serial0/1/1
O       192.168.1.36/30 [110/128] via 192.168.1.42, 02:14:12, Serial0/2/1
                        [110/128] via 192.168.1.33, 02:14:12, Serial0/1/1
C       192.168.1.40/30 is directly connected, Serial0/2/1
L       192.168.1.41/32 is directly connected, Serial0/2/1
```

Router Admin-TI:

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.0.0/24 is variably subnetted, 4 subnets, 3 masks
O       192.168.0.0/25 [110/65] via 192.168.1.41, 02:14:41, Serial0/2/1
O       192.168.0.128/26 [110/65] via 192.168.1.41, 02:14:41, Serial0/2/1
C       192.168.0.192/26 is directly connected, GigabitEthernet0/0/0.30
L       192.168.0.193/32 is directly connected, GigabitEthernet0/0/0.30
     192.168.1.0/24 is variably subnetted, 7 subnets, 3 masks
C       192.168.1.0/27 is directly connected, GigabitEthernet0/0/0.40
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0/0.40
O       192.168.1.32/30 [110/128] via 192.168.1.41, 02:14:41, Serial0/2/1
                        [110/128] via 192.168.1.37, 02:14:41, Serial0/2/0
C       192.168.1.36/30 is directly connected, Serial0/2/0
L       192.168.1.38/32 is directly connected, Serial0/2/0
C       192.168.1.40/30 is directly connected, Serial0/2/1
L       192.168.1.42/32 is directly connected, Serial0/2/1
```

Router Principal:

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.0.0.0/30 is directly connected, Serial0/1/0
L       10.0.0.1/32 is directly connected, Serial0/1/0
     192.168.0.0/24 is variably subnetted, 3 subnets, 2 masks
O       192.168.0.0/25 [110/65] via 192.168.1.34, 02:15:09, Serial0/1/1
O       192.168.0.128/26 [110/65] via 192.168.1.34, 02:15:09, Serial0/1/1
O       192.168.0.192/26 [110/65] via 192.168.1.38, 02:15:09, Serial0/2/0
     192.168.1.0/24 is variably subnetted, 6 subnets, 3 masks
O       192.168.1.0/27 [110/65] via 192.168.1.38, 02:15:09, Serial0/2/0
C       192.168.1.32/30 is directly connected, Serial0/1/1
L       192.168.1.33/32 is directly connected, Serial0/1/1
C       192.168.1.36/30 is directly connected, Serial0/2/0
L       192.168.1.37/32 is directly connected, Serial0/2/0
O       192.168.1.40/30 [110/128] via 192.168.1.38, 02:15:09, Serial0/2/0
                        [110/128] via 192.168.1.34, 02:15:09, Serial0/1/1
```

4. **DNS:**
   4.1. ping mail.nexacapital.com

Desde una PC Alberto en RH:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping mail.nexacapital.com

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=2ms TTL=126
Reply from 192.168.1.2: bytes=32 time=31ms TTL=126
Reply from 192.168.1.2: bytes=32 time=17ms TTL=126
Reply from 192.168.1.2: bytes=32 time=29ms TTL=126

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 31ms, Average = 19ms
```

5. **DHCP:**
   5.1. show ip dhcp binding

Router Fin-RH:

IP address	Client-ID/ Hardware address	Lease expiration	Type
192.168.0.2	0001.C772.09C7	--	Automatic
192.168.0.5	0001.435A.695E	--	Automatic
192.168.0.4	00D0.970B.EA30	--	Automatic
192.168.0.3	0002.1630.2422	--	Automatic
192.168.0.6	0090.0C87.105A	--	Automatic
192.168.0.7	000D.BD34.DA17	--	Automatic
192.168.0.8	000A.F349.A64E	--	Automatic
192.168.0.131	0000.0CC1.1624	--	Automatic
192.168.0.130	000B.BE2B.2420	--	Automatic

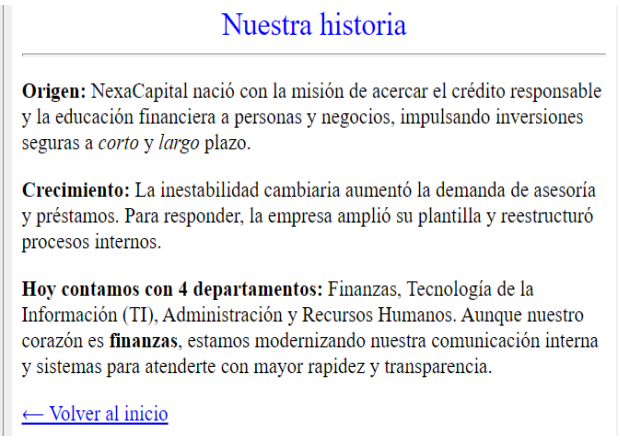
Router Admin-TI:

IP address	Client-ID/ Hardware address	Lease expiration	Type
192.168.0.195	0007.ECA9.3834	--	Automatic
192.168.0.194	00E0.F76B.0EAA	--	Automatic
192.168.1.3	0060.2F1E.1A47	--	Automatic
192.168.1.4	0001.960E.C0C7	--	Automatic
192.168.1.5	0090.214E.C9AA	--	Automatic
192.168.1.7	000B.BE92.00B8	--	Automatic
192.168.1.6	0002.16B3.84E2	--	Automatic

6. HTTP:

6.1. Navega a http://www.nexacapital.com o http://<IP_del_servidor> → carga OK desde todas las VLANs.

Desde el browser de la PC Sebas en Admin:



7. Correo (SMTP/POP3):

7.1. Envío y recibo de correos.

Se pueden enviar mas no recibir, problema con la configuración y validación interna de POP3.

8. Salida a ISP y BGP:

8.1. show ip bgp summary → Established con el vecino del ISP.

Router Principal:

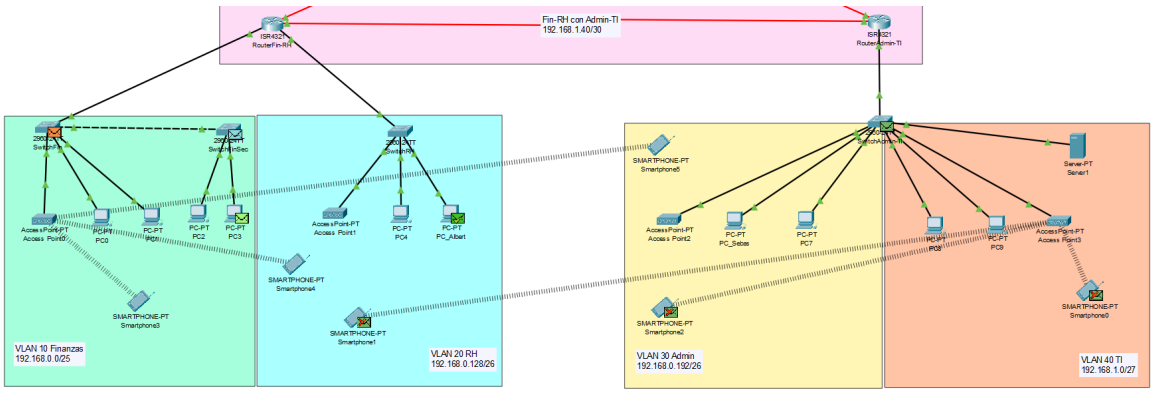
```
BGP router identifier 192.168.1.37, local AS number 200
BGP table version is 18, main routing table version 6
8 network entries using 1056 bytes of memory
8 path entries using 416 bytes of memory
0/0 BGP path/bestpath attribute entries using 0 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 1) using 32 bytes of memory
BGP using 1528 total bytes of memory
BGP activity 7/0 prefixes, 8/0 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.0.0.2        4   100     144     143       18    0    0 01:17:41        4
```

Router Liberty:

```
BGP router identifier 10.0.0.2, local AS number 100
BGP table version is 15, main routing table version 6
7 network entries using 924 bytes of memory
7 path entries using 364 bytes of memory
7/7 BGP path/bestpath attribute entries using 1288 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 1) using 32 bytes of memory
BGP using 2632 total bytes of memory
BGP activity 7/0 prefixes, 7/0 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.0.0.1        4   200     157     145       15    0    0 01:18:23        4
```

9. Captura de paquetes (evidencias):

9.1. Simulation en Packet Tracer



Los paquetes circulan bien entre los diferentes departamentos de la empresa.

B. Análisis del funcionamiento:

- **Rendimiento básico:** tiempos de respuesta de *ping* en PT ~1–2 ms; pérdida 0%.
- **Tablas de enrutamiento coherentes:** sin rutas superpuestas o faltantes.
- **Aislamiento L2:** equipos de VLAN distintos no se alcanzan si **no** hay routing (prueba opcional desconectando OSPF).
- **Seguridad de acceso:** puertos no usados en *administratively down*; Port-Security sin violaciones.

C. Comparación con lo esperado:

Prueba	Resultado	Evidencia	¿Cumple?
Ping PC-Fin → GW VLAN10	Ping entre todos los depts	Simulation + purebas	Sí
Inter-VLAN PC-Fin → PC-RH	Éxito	Pruebas	Sí
DHCP (PC-Admin)	IP/máscara/GW/DNS correctos	Pruebas	Sí
DNS mail.nexacapital.com	resuelve a 192.168.1.2 y sirve correctamente	Pruebas	Sí
HTTP Intranet	carga desde todas las VLAN	screenshot	Sí
SMTP/POP3	envío bien, recpecion mal	Pruebas	Sí y No
OSPF vecinos	FULL	show ip ospf neighbor	Sí
BGP con ISP	Hay conexion, no ping	show ip bgp summary	Sí y No
Seguridad switches	sin violaciones	Pruebas	Sí
ACL	Planteado pero no implementado	--	--

Durante la batería de pruebas se confirmó la conectividad interna: hubo ping exitoso entre todos los departamentos y tráfico inter-VLAN sin pérdidas; DHCP asignó correctamente IP, máscara, gateway y DNS, y DNS resolvió *mail.nexacapital.com* a 192.168.1.2; la intranet HTTP cargó desde todas las VLAN. En OSPF los vecinos quedaron en estado FULL, evidenciando un enrutamiento interno estable. Dos puntos quedaron a medias: en correo, el SMTP envía, pero la recepción por POP3 falló en algunos casos; y en la salida al ISP, BGP está establecido (hay sesión y rutas), pero no se logra ping, lo que sugiere un ajuste pendiente (p. ej.,

redistribución/ACLs/NAT según el escenario). La seguridad en switches no mostró violaciones y las ACL quedaron solo planificadas, no implementadas.

Conclusiones y recomendaciones:

Reflexión crítica sobre lo aprendido.

El proyecto nos obligó a diseñar "como en producción": pensar en capas (acceso–distribución–core), dimensionar con VLSM y justificar cada protocolo por su función. Aprendimos a integrar servicios (DHCP, DNS, HTTP y correo) con el plano de control (OSPF/BGP) y a validar todo con evidencia: tablas de enrutamiento, vecinos OSPF en FULL, pruebas de resolución de nombres y tráfico entre VLANs. También vimos el valor de la documentación y los estándares (nomenclatura, descripciones, plantillas de configuración y pruebas), porque cada pequeño detalle, por ejemplo, un network que falta en OSPF, puede romper un caso de uso crítico aunque "todo lo demás" parezca estar bien.

Principales hallazgos.

La segmentación por VLAN funcionó correctamente y el enrutamiento inter-VLAN fue estable; DHCP asignó parámetros válidos y DNS resolvió nombres internos sin problemas. Identificamos dos puntos de fricción: (1) en correo, el envío por SMTP fue exitoso, pero la recepción POP3 falló de forma intermitente, lo que apunta a una combinación de parámetros de servidor/cliente (dominio, buzones/usuarios, puertos/ACL locales); (2) con el ISP, BGP estableció vecindad, pero no se logró hacer ping desde LAN hacia la 10.0.0.0/30. La causa más probable es de alcance de rutas: el enlace 10.0.0.0/30 no fue anunciado por OSPF hacia los routers de distribución (o no existía default inyectada hacia ellos), por lo que las estaciones no tenían ruta específica/implícita para llegar a 10.0.0.2. Es un hallazgo valioso: una sesión BGP "Established" no garantiza por sí sola la conectividad de extremo a extremo si el plano IGP no publica todos los prefijos requeridos o si falta una ruta por defecto.

Aplicabilidad en entornos reales.

La arquitectura adoptada es directamente trasladable a pymes en crecimiento: segmentación por áreas (Finanzas, RRHH, Admin, TI), puertas de enlace en subinterfaces (router-on-a-stick), OSPF para la convergencia interna y BGP para la peering con ISP/sedes. Los servicios básicos (DNS, DHCP, intranet y correo) y el hardening de switches (consola/VTY, enable secret, Port-Security, BPDU Guard) cubren el "mínimo viable" de operación segura. Además, el diseño facilita la evolución: mover el correo a la nube, agregar más VLANs o crecer a HSRP/VRRP en gateways se hace sin rediseñar todo.

Mejoras al diseño o configuración.

Técnicamente, proponemos:

- Rutas y redistribución: anunciar explícitamente el enlace 10.0.0.0/30 en OSPF o propagar una ruta por defecto desde el core a distribución (por ejemplo, BGP default-originate en el ISP y redistribute bgp→OSPF en el principal), de modo que las LAN conozcan cómo llegar al /30 y al exterior.

- Correo: verificar buzones/usuarios, dominio y puertos; probar POP3/IMAP con telnet o openssl s_client, revisar ACL locales y, si aplica, NAT/inspecciones.

- Seguridad: añadir SSH (deshabilitar Telnet), AAA/privilegios por usuario, OSPF authentication, control de tormentas, DHCP Snooping + DAI, y listas de control entre VLANs con la política de "mínimo privilegio".

- Alta disponibilidad y operación: HSRP/VRRP para gateways, EtherChannel en troncales, NTP/Syslog/SNMPv3 para observabilidad, respaldos automáticos de configuración, y plantillas de "golden config".

- Escalabilidad: prever IPv6 dual-stack, QoS para voz/vídeo y segmentación adicional (guest Wi-Fi, IoT) con VLANs dedicadas.

Buenas prácticas para futuros trabajos similares.

1) Diseñar con "pruebas primero": definir casos de prueba y criterios de aceptación antes de cablear/configurar.
2) Mantener un catálogo de prefijos (qué IGP/BGP debe ver cada red) y auditar al final.
3) Versionar configuraciones y usar plantillas consistentes (nombres, descripciones, políticas de seguridad).
4) Documentar topologías L2/L3 y flujos de servicio (por ejemplo, correo y DNS) con sus dependencias.
5) Aislar entornos de laboratorio y replicar fallos allí antes de tocar producción.
6) Medir: recopilar KPIs simples (pérdida, latencia, convergencia OSPF, uptime de vecinos BGP) y anexar capturas/outputs como evidencia. Con estas prácticas, la próxima iteración será más rápida, segura y predecible, y la transición a producción quedará respaldada por datos y no solo por percepciones.

Referencias bibliográficas

Cisco Systems. (2018). *Cisco Enterprise Architecture*. Cisco Press.

Cisco Systems. (2020). *Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide*. Cisco Press.

Droms, R. (1997). RFC 2131: Dynamic Host Configuration Protocol. https://doi.org/10.17487/RFC2131

ISO. (2013). ISO/IEC 27001: Information technology — Security techniques — Information security management systems — Requirements. International Organization for Standardization.

Kurose, J. F., & Ross, K. W. (2021). *Computer Networking: A Top-Down Approach* (8th ed.). Pearson.

Mockapetris, P. (1987). RFC 1034: Domain Names - Concepts and Facilities. https://doi.org/10.17487/RFC1034

NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology.

Odom, W. (2020). *CCNA 200-301 Official Cert Guide, Volume 2*. Cisco Press.

Paniagua, M., & Alvarado, J. (2019). Protección de datos personales en Costa Rica: Ley 8968 y su aplicación. *Revista de Derecho Informático*, 12(2), 45–57.

Scarfone, K., & Hoffman, P. (2009). Guidelines on Firewalls and Firewall Policy. NIST Special Publication 800-41 Revision 1. https://doi.org/10.6028/NIST.SP.800-41r1