

# Proyecto Redes II

**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.**

David Abarca Chaves (202001610152)  
Alberto Álvarez Navarro ( 20210110651)  
Sebastián Chaves Solano (20200120941)  
Santiago Ramírez Elizondo (202401112941)



# Introducción

NexaCapital, empresa reconocida en préstamos e inversiones, ha experimentado un crecimiento acelerado con la creación de 4 departamentos: Finanzas, TI, Administración y RRHH.

El sistema de red interno actual es básico y presenta vulnerabilidades que comprometen datos de clientes y empleados.

Para mejorar la comunicación interna, seguridad y escalabilidad, se propone implementar VLANs, ACLs y servicios como DNS, DHCP, correo y red corporativa.

# Objetivos

## 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.

El presente proyecto busca implementar una infraestructura de red robusta, segura, escalable y automatizada para NexaCapital, apoyando su expansión organizacional y el incremento en la demanda de servicios financieros. El diseño se fundamenta en un modelo jerárquico de tres capas (capa de acceso, capa de distribución y capa núcleo), donde la capa de distribución agrega el tráfico de los switches de acceso para luego ser encaminado a la capa núcleo, alineándose con prácticas consolidadas en diseño de redes empresariales

---



# Alcance del Proyecto

# Conceptos importantes

## Fundamentos de Redes

### Modelos de Referencia

- OSI: 7 capas para estandarizar funciones de comunicación.
- TCP/IP: 4 capas, base de Internet y redes empresariales, incluye protocolos como TCP, UDP, DNS, DHCP.

### Switching y Enrutamiento

- Switching: Transfiere datos en una LAN, mejora rendimiento (Capa 2 OSI).
- Enrutamiento: Comunica redes diferentes, define la mejor ruta para el tráfico (Capa 3 OSI).

### VLANs

- Segmentan la red física en redes lógicas aisladas.
- Mejoran la seguridad y el uso del ancho de banda.
- Aplicación en NexaCapital: una VLAN por departamento.

# Conceptos importantes

## Servicios y Seguridad

### Servicios de Red

- DNS: Traduce nombres de dominio a direcciones IP.
- DHCP: Asigna IPs automáticamente.
- Correo corporativo: Comunicación interna y externa segura.

### Seguridad (ACLs)

- Filtran tráfico por IP, puerto y protocolo.
- Protegen datos sensibles y evitan accesos no autorizados.

### Arquitectura Jerárquica

- Capas: acceso, distribución y núcleo.
- Facilita escalabilidad y administración eficiente.

### Normativas y Estándares

- Ley 8968 (Costa Rica) – protección de datos personales.
- ISO 27001 y NIST – buenas prácticas en seguridad informática.

# Aspectos Clave del Proyecto de Red – NexaCapital

- Diseño jerárquico y escalable: capas de acceso, distribución y núcleo.
- VLANs por departamento (Finanzas, Servicio al Cliente, TI, Administración, RRHH, Gerencia) con subredes planificadas y enrutamiento interno eficiente.
- Servicios de red internos: DNS, DHCP, correo corporativo e intranet.
- Ciberseguridad básica: ACLs entre VLANs, firewalls perimetrales/locales, control de acceso físico y lógico a infraestructura.
- Escalabilidad planificada: espacio en subredes para futuros departamentos, usuarios o sedes.
- Documentación técnica completa: diagramas, direccionamiento IP, configuraciones y políticas de seguridad.

No incluye: equipos personales, servicios en la nube, soluciones avanzadas de ciberseguridad ni soporte más allá de 3 años.

# Soluciones Tecnológicas Evaluadas:

## Solución

Red tradicional con VLANs, ACLs, servidores locales

Infraestructura híbrida (local + servicios en la nube)

## Características

Infraestructura física centralizada con servicios DNS, DHCP, correo y red corporativa en servidores propios. Segmentación por VLANs y control mediante ACLs.

Parte de los servicios (como correo y almacenamiento) en la nube, como Microsoft 365 o Google Workspace. DNS/DHCP internos. Red física con VLANs.

## Ventajas

Mayor control interno, personalización total, sin dependencia de terceros.

Reducción en mantenimiento, alta disponibilidad, acceso remoto sencillo.

## Desventajas

Mayor inversión inicial en hardware, requiere mantenimiento técnico continuo.

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.

## Requerimientos técnicos:

### Análisis de acuerdo a la arquitectura de red:

Departamentos	Total de trabajadores (Conexión 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
<b>Total de dispositivos:</b>	<b>94</b>	<b>113</b>	<b>207</b>

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	



## B. Hardware

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, Escalabilidad y Sostenibilidad**

## **– NexaCapital**

### **Compatibilidad con sistemas existentes**

- Infraestructura actual básica, sin segmentación ni servidores dedicados.
- PCs y dispositivos existentes compatibles con Ethernet y VLANs.
- Migración facilitada por ausencia de sistemas heredados complejos.
- Reuso de hardware vigente; reemplazo solo de equipos no gestionables.

### **Escalabilidad y sostenibilidad tecnológica**

- Diseño modular por VLANs para fácil integración de nuevos departamentos.
- Subredes expansibles con direccionamiento IP planificado.
- Servidores con capacidad de virtualización para nuevos servicios.
- Preparado para migrar a la nube en el futuro sin afectar operaciones.
- Políticas de mantenimiento preventivo y actualizaciones periódicas.

# Factibilidad Económica y Financiera:

Componente	Modelo	Unidades	Precio por	Total	Fuente
<b>Dispositivos principales</b>					
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
<b>Cableado Estructurado</b>					
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
<b>Servicios Profesionales</b>					
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
<b>Presupuesto final total:</b>			\$ 32,162.62	€ 16,081,310.00	

- Fuentes de financiamiento:**

La empresa podría financiar este proyecto mediante una combinación de:

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

# Factibilidad Económica y Financiera:

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

Retorno o beneficios esperados:

1. Económicos:

- a. Reducción de pérdidas por fallos de red y tiempos muertos.
- b. Aumento de productividad interna (conectividad, colaboración).
- c. Mejor aprovechamiento de sistemas de información y bases de datos.
- d. Reducción de costos de soporte externo no planificado.
- e. Escalabilidad sin necesidad de rediseños costosos en el corto plazo.

1. Sociales:

- a. Mejora en la comunicación interdepartamental, especialmente en atención al cliente.
- b. Ambiente laboral más eficiente y tecnológico.
- c. Facilita el teletrabajo parcial o trabajo remoto seguro.

1. Ambientales:

- a. Uso eficiente de energía mediante switches PoE, UPS inteligentes y menos cantidad de hardware (por consolidación)
- b. Menor necesidad de traslados físicos o impresiones, promoviendo procesos digitales.
- c. 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)	

# Riesgos Generales

## 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

## Terceros Afectados – Proyecto de Red NexaCapital

1. Clientes: Beneficio indirecto con mayor protección de datos y servicio más ágil y confiable.
2. Funcionarios internos: Impacto directo por adaptación a nuevas tecnologías y procedimientos (requiere capacitación).
3. Proveedores tecnológicos: Participación en venta, instalación y soporte de equipos y servicios.
4. Instituciones gubernamentales y regulatorias: Impacto positivo al verificar el cumplimiento de normativas de seguridad y tratamiento de datos.

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 la 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.

# Subneteo, Direcccionamiento IP y Orden de Red – NexaCapital

Red principal: 192.168.0.0/24 (máx. 254 hosts) – Aplicación de VLSM

- Finanzas → 192.168.0.0/25 (255.255.255.128)
  - Rango: .0 – .127 | Gateway: .1 | 110 hosts
- RRHH → 192.168.0.128/26 (255.255.255.192)
  - Rango: .128 – .191 | Gateway: .129 | 44 hosts
- TI → 192.168.0.192/26 (255.255.255.192)
  - Rango: .192 – .255 | Gateway: .193 | 31 hosts
- Administración → 192.168.1.0/27 (255.255.255.224)
  - Rango: .0 – .31 | Gateway: 192.168.1.1 | 22 hosts

Enlaces punto a punto:

- 192.168.1.32/30 – 192.168.1.36/30 – 192.168.1.40/30

Salida ISP (BGP): 10.0.0.0/30

Notas:

- Uso de wildcards para OSPF y ACLs.
- Primera IP = gateway, última IP = broadcast.

Dept.	Hosts Req. (Permitidos)	Máscara de Subred/bits	Wildcard	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 – NexaCapital

## Topología

- Core: 1 Router Principal.
- Distribución: 2 routers (Finanzas–RRHH a la izquierda y Administración–TI a la derecha).
- Acceso: switches y APs por VLAN.

## Segmentación VLAN

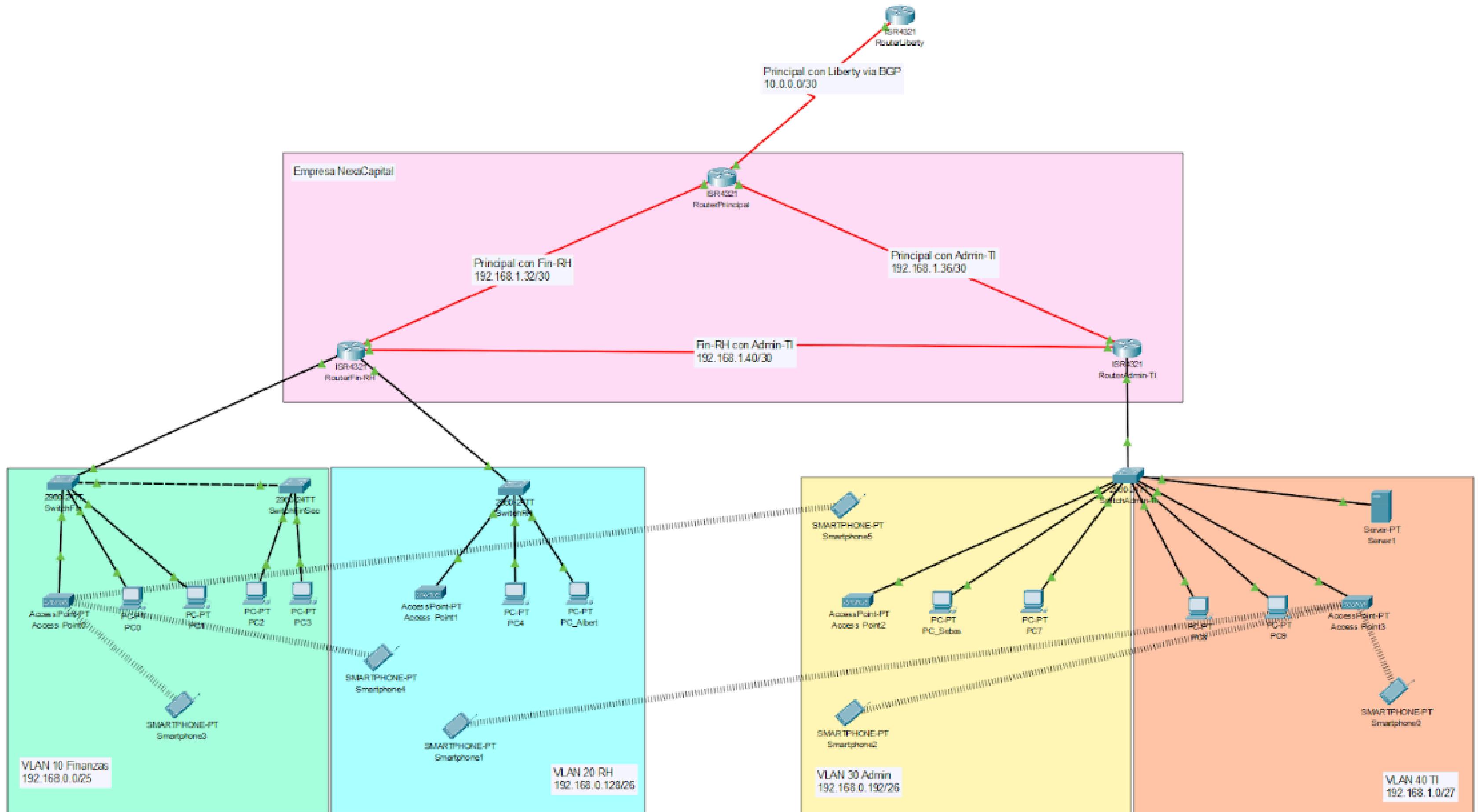
- VLAN10 Finanzas → 192.168.0.0/25
- VLAN20 RRHH → 192.168.0.128/26
- VLAN30 Administración → 192.168.0.192/26
- VLAN40 TI → 192.168.1.0/27
- Gateways en .1 de cada subred, en subinterfaces de los routers.
- Switches troncales para enrutamiento inter-VLAN.

## Conexiones y protocolos

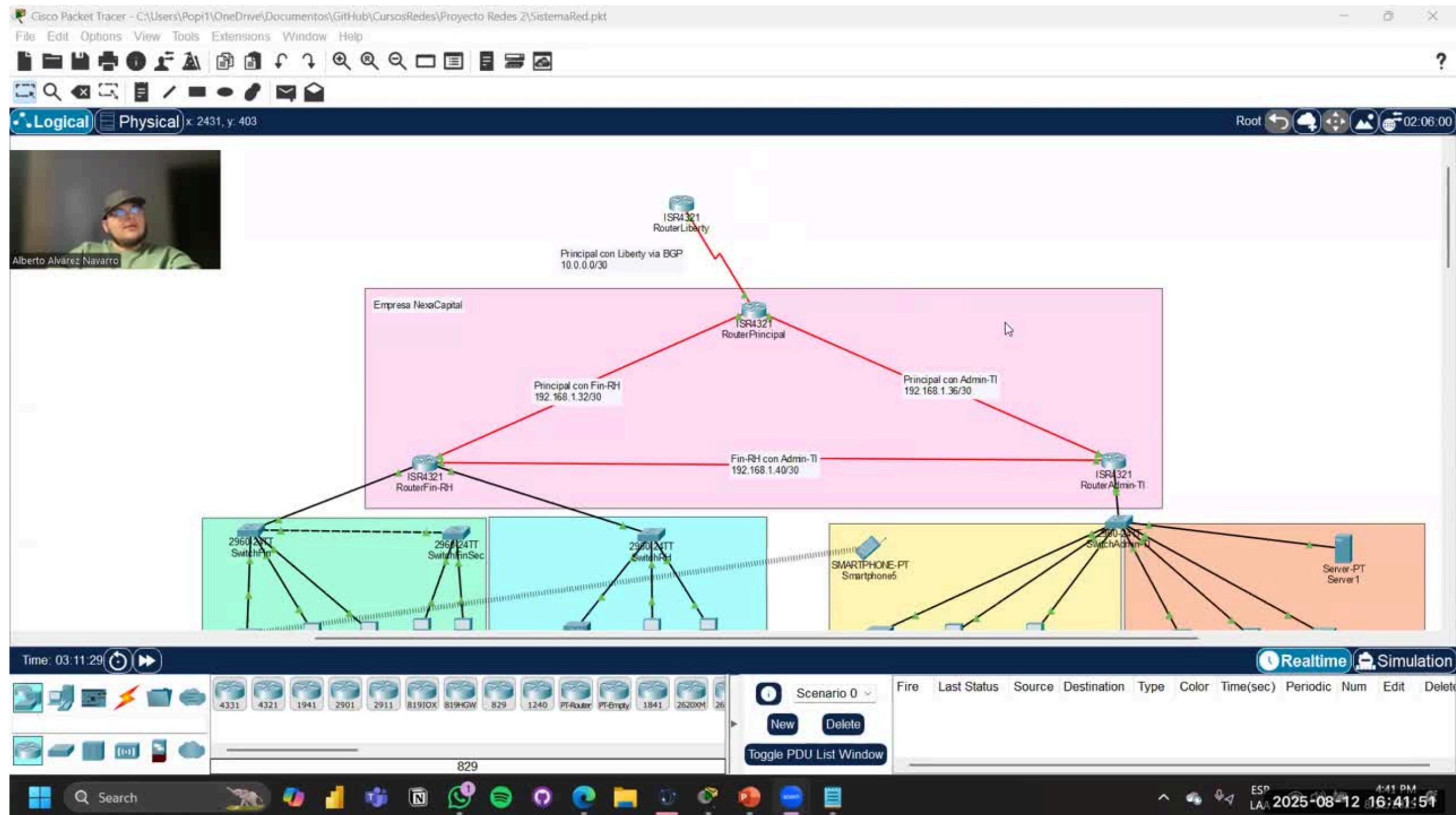
- Enlaces /30 (192.168.1.32/30, 192.168.1.36/30, 192.168.1.40/30) con OSPF para redundancia y anuncio de redes.
- Router Principal → ISP por 10.0.0.0/30 usando BGP, redistribuyendo ruta por defecto.

## Servicios y conectividad

- APs extienden WiFi segmentado por VLAN.
- Servidor en VLAN TI (DNS, HTTP, correo) accesible desde todos los departamentos.



# Presentación de Video



# Configuración de Routers y Switches – NexaCapital

Routers de distribución (Fin-RRHH / Admin-TI)

- Enrutamiento inter-VLAN (router-on-a-stick): subinterfaces con encapsulation dot1Q para VLAN10, 20, 30, 40.
- Gateways: .1, .129, .193 y 192.168.1.1.
- Enlaces WAN /30 en interfaces Serial (bandwidth 1544).
- OSPF (router ospf 1, network ... area 0) para anunciar subredes y enlaces.
- Pools DHCP (ip dhcp pool, network, default-router, dns-server 192.168.1.2).
- Comandos de optimización: no ip domain-lookup, description.

Router Principal e ISP (Liberty)

- Conexión ISP: 10.0.0.0/30 en Serial0/1/0.
- BGP (router bgp, neighbor ... remote-as).
- Redistribución OSPF ↔ BGP para rutas internas y externas.
- Anuncio enlaces /30 internos por OSPF.
- router-id 1.1.1.1 para estabilidad del proceso.

# Configuración de Routers y Switches – NexaCapital

## Switches de acceso

- Creación de VLANs (10, 20, 30, 40).
- Puertos de usuario: switchport mode access, switchport access vlan X.
- Trunks hacia routers/switches: switchport mode trunk, switchport trunk allowed vlan ..., nonegotiate.
- Seguridad: STP PortFast, BPDU Guard, enable secret, contraseñas en consola y VTY, logging synchronous.

## Servicios internos (Servidor 192.168.1.2)

- DNS: registros A y CNAME (www.nexacapital.com, nexacapital.com).
- Correo: SMTP y POP3 (mail.nexacapital.com).
- Intranet: HTTP Server para páginas corporativas.
- DHCP en routers apunta a dns-server 192.168.1.2 para integrar resolución de nombres.

# VLAN'S

show vlan brief

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	

# Enlaces Trunk

show interfaces trunk

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			

# OSPF

show ip ospf neighbor

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

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
```

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
```

show ip route

# DNS

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
```

# DHCP

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

# Asignación Dinámica

PC Alberto en RH:

Interface	FastEthernet0
IP Configuration	
<input checked="" type="radio"/> DHCP	<input type="radio"/> Static
IPv4 Address	192.168.0.131
Subnet Mask	255.255.255.192
Default Gateway	192.168.0.129
DNS Server	192.168.1.2

PC Sebas en Admin:

Interface	FastEthernet0
IP Configuration	
<input checked="" type="radio"/> DHCP	<input type="radio"/> Static
IPv4 Address	192.168.0.194
Subnet Mask	255.255.255.192
Default Gateway	192.168.0.193
DNS Server	192.168.1.2

# HTTP

Navega a <http://www.nexacapital.com> o [http://<IP\\_del\\_servidor>](http://<IP_del_servidor>) → carga OK desde todas las VLANs.

Desde el browser de la PC Sebas en Admin:



The screenshot shows a Windows desktop environment. A taskbar at the bottom has several icons, including a browser window titled "PC\_Sebas". The browser window displays the NexaCapital website. The page title is "NexaCapital". The main content area says "Bienvenido a **NexaCapital**, un organismo reconocido por sus **servicios de préstamos** y por la **enseñanza de finanzas** para inversión a corto y largo plazo. Crecemos de la mano de nuestros clientes, ofreciendo claridad y acompañamiento en cada decisión." Below this, it says "La reciente volatilidad del dólar incrementó la demanda y nos llevó a ampliar nuestro equipo y departamentos para servirte mejor." Under "Quick Links", there are links to "Nuestra historia", "Contacto", and "Logo". To the right of the browser window, there is a sidebar with a blue header "Nuestra historia". The content under this header includes: "Origen: NexaCapital nació con la misión de acercar el crédito responsable y la educación financiera a personas y negocios, impulsando inversiones seguras a *corto* y *largo* plazo.", "Crecimiento: La inestabilidad cambiaria aumentó la demanda de asesoría y préstamos. Para responder, la empresa amplió su plantilla y reestructuró procesos internos.", and "Hoy contamos con 4 departamentos: Finanzas, Tecnología de la Información (TI), Administración y Recursos Humanos. Aunque nuestro corazón es **finanzas**, estamos modernizando nuestra comunicación interna y sistemas para atenderte con mayor rapidez y transparencia.". At the bottom of this sidebar is a link "[← Volver al inicio](#)".

Nuestra historia

**Origen:** NexaCapital nació con la misión de acercar el crédito responsable y la educación financiera a personas y negocios, impulsando inversiones seguras a *corto* y *largo* plazo.

**Crecimiento:** La inestabilidad cambiaria aumentó la demanda de asesoría y préstamos. Para responder, la empresa amplió su plantilla y reestructuró procesos internos.

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

[← Volver al inicio](#)

# Salida a ISP y BGP

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

# Comparación con lo esperado

Funcionó correctamente:

- Conectividad interna: Ping exitoso entre todos los departamentos y tráfico inter-VLAN sin pérdidas.
- DHCP: Asignación correcta de IP, máscara, gateway y DNS.
- DNS: Resolución de mail.nexacapital.com → 192.168.1.2.
- Intranet HTTP: Accesible desde todas las VLAN.
- OSPF: Vecinos en estado FULL, enrutamiento estable.
- Seguridad en switches: Sin alertas ni violaciones.

Pendiente de corrección:

- Correo electrónico: SMTP funcional, POP3 con fallos intermitentes.
- Salida al ISP: BGP establecido y con rutas, pero sin conectividad (posible ajuste de redistribución, ACLs o NAT).
- ACLs: Planificadas pero no implementadas.

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, recepcion mal	Pruebas	Sí y No
OSPF vecinos	FULL	show ip ospf neighbor	Sí
BGP con ISP	Hay conexión, no ping	show ip bgp summary	Sí y No
Seguridad switches	sin violaciones	Pruebas	Sí
ACL	Planteado pero no implementado	--	--

# Conclusiones y Recomendaciones – NexaCapital



## Reflexión crítica

- El proyecto obligó a diseñar con mentalidad de producción: jerarquía (acceso–distribución–core), VLSM justificado, protocolos por función.
- Se integraron servicios (DHCP, DNS, HTTP, correo) con enrutamiento (OSPF/BGP) y se validó con evidencias: tablas de enrutamiento, vecinos OSPF en FULL, pruebas de resolución de nombres y conectividad entre VLANs.
- La documentación y estándares fueron clave: un solo network ausente en OSPF puede comprometer servicios críticos.

## Principales hallazgos

1. VLAN y enrutamiento inter-VLAN: Estables y funcionales.
2. DHCP/DNS: Configuración correcta y operativa.
3. Correo: SMTP operativo, POP3 intermitente (posibles ajustes en usuarios, dominio, puertos, ACLs).
4. BGP: Vecindad establecida, pero sin ping al ISP (probable falta de anuncio del /30 o ruta por defecto en OSPF).

# Conclusiones y Recomendaciones – NexaCapital

## Aplicabilidad real

- Diseño adaptable a pymes: segmentación por áreas, router-on-a-stick, OSPF interno, BGP para ISP.
- Servicios básicos y seguridad mínima viable (DNS, DHCP, intranet, correo, hardening de switches).
- Escalable para correo en la nube, más VLANs o gateways redundantes sin rediseñar todo.

## Mejoras propuestas

- Rutas: Anunciar explícitamente 10.0.0.0/30 en OSPF o propagar ruta por defecto desde core a distribución.
- Correo: Revisar parámetros POP3/IMAP, ACLs y NAT; pruebas con telnet u openssl s\_client.
- Seguridad: Implementar SSH, AAA, autenticación OSPF, DHCP Snooping, ACLs por mínimo privilegio.
- Alta disponibilidad: HSRP/VRRP, EtherChannel, NTP/Syslog/SNMPv3, respaldos automáticos.
- Escalabilidad: IPv6, QoS, VLANs adicionales (guest Wi-Fi, IoT).

## Buenas prácticas

- Diseñar con “pruebas primero” y criterios claros de aceptación.
- Mantener catálogo de prefijos y auditar visibilidad en IGP/BGP.
- Versionar configuraciones con plantillas consistentes.
- Documentar topologías y flujos de servicio con dependencias.
- Replicar fallos en laboratorio antes de producción.
- Medir KPIs simples (pérdida, latencia, convergencia, uptime BGP) y respaldar con evidencias.

Gracias por su  
atención