



# Diseño y Arquitectura de Red para el Campus Universitario JNA

Este documento presenta el diseño técnico de una infraestructura de red robusta y segura para el Campus Universitario JNA. Abordaremos la arquitectura fundamental, la planificación de direcciones IP, el enrutamiento, las políticas de seguridad y la gestión de acceso, elementos cruciales para un entorno universitario moderno.

## 1. Arquitectura de Red y Alta Disponibilidad

El diseño de la red del campus JNA se fundamenta en un modelo jerárquico de dos capas, conocido como "Colapso del Core en Distribución". Esta estrategia optimiza la latencia en la transmisión de datos y simplifica la gestión de la infraestructura, al consolidar las funciones de core y distribución.

### Modelo de dos capas

La fusión de las capas de núcleo y distribución reduce la complejidad y mejora la eficiencia operativa.

### Optimización de Latencia

Al disminuir los dispositivos intermedios, se logra una reducción significativa en la latencia, crucial para aplicaciones sensibles.

### Facilidad de Administración

Un diseño más compacto significa menos puntos de configuración y monitorización, simplificando la operación diaria de la red.

## 1.1. Topología de Enlaces Troncales con EtherChannel

Para garantizar un ancho de banda óptimo y una resiliencia superior, hemos implementado EtherChannel utilizando el protocolo LACP (Link Aggregation Control Protocol, 802.3ad). Esta tecnología agrega múltiples enlaces físicos entre la capa de distribución y acceso, creando un único canal lógico con mayor capacidad y redundancia.





### Agregación de Enlaces

Cada EtherChannel proporciona un ancho de banda de hasta 200 Mbps en modo Full Duplex, lo que asegura un rendimiento elevado para el tráfico intenso del campus.



### Redundancia Incorporada

En caso de fallo de uno o varios cables físicos, el tráfico se redistribuye automáticamente entre los enlaces restantes, manteniendo la conectividad sin interrupciones.

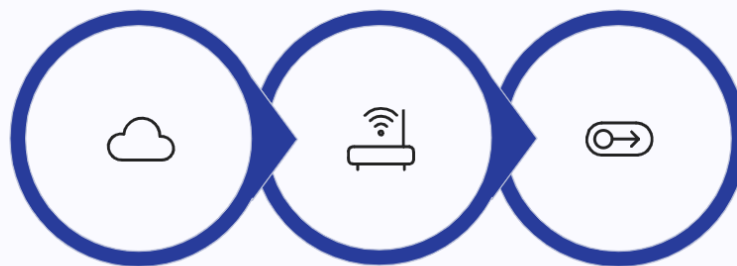


### Gestión de VLANs (SVIs)

La distribución de las VLANs de usuarios se realiza a través de SVIs (Switch Virtual Interfaces) en los switches multicapa (DSW1, DSW2, DSW3), que actúan como Default Gateways para sus respectivas VLANs.

## Topología General de la Red del Campus JNA

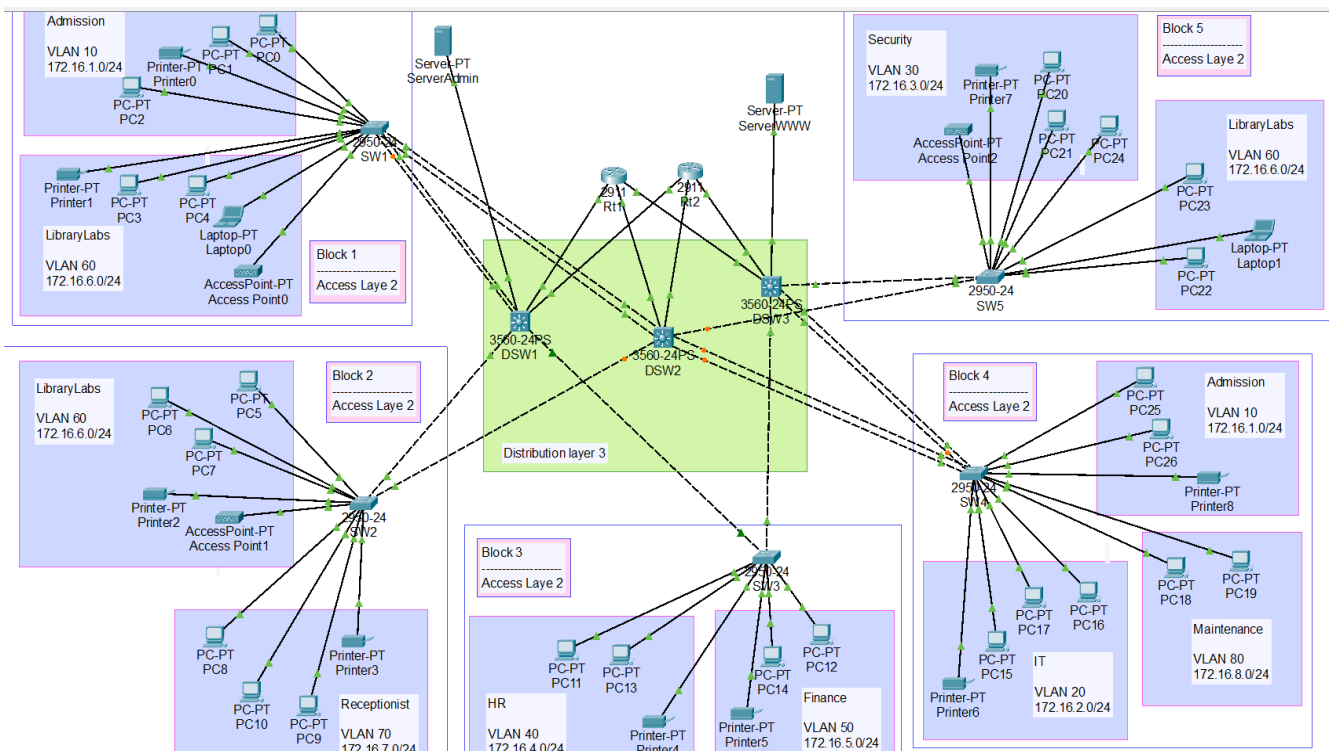
La red del Campus JNA implementa una topología de red jerárquica de tres capas, que incluye una capa de acceso, una capa de distribución y una capa de núcleo, garantizando redundancia y escalabilidad desde la conexión a Internet hasta los dispositivos finales de los usuarios. Esta estructura optimiza el flujo de tráfico, la seguridad y la facilidad de gestión.



Núcleo  
Exterior

Enrutamiento  
o Edge

Distribución  
y Acceso



# Implementación Técnica Destacada

Hemos puesto especial énfasis en la implementación de tecnologías clave que aseguran la resiliencia y el rendimiento de la red del campus.

## Alta Disponibilidad (EtherChannel)

Para maximizar el ancho de banda y garantizar la redundancia entre las capas de distribución y acceso, se configuraron Port-Channels (LACP). Un ejemplo es el enlace entre DSW1 y SW1, que utiliza los puertos Fa0/23 y Fa0/24 bajo el Port-channel 1, brindando tolerancia a fallos.

## Enrutamiento Dinámico (EIGRP)

Se seleccionó EIGRP (AS 100) por su rápida convergencia y su eficiencia en entornos Cisco. Este protocolo propaga automáticamente las redes de las VLANs y los enlaces entre routers, asegurando que cualquier fallo de enlace sea detectado y corregido en milisegundos, minimizando el tiempo de inactividad.

# Esquema de Direccionamiento IP y Enlaces

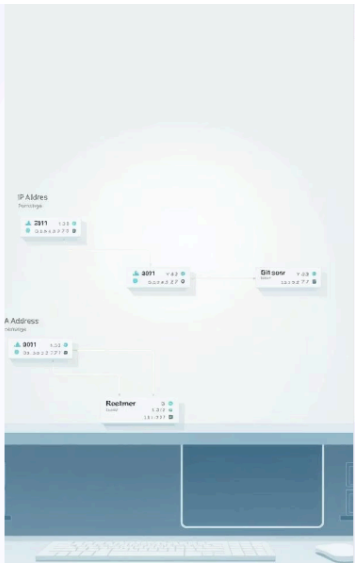
El direccionamiento IP ha sido cuidadosamente planificado para optimizar el enrutamiento y garantizar la segregación de la red.

### Backbone

- Conexiones redundantes entre Routers (Rt1, Rt2) y Switches de Distribución (DSW1-3).
- Utiliza el rango 10.10.1.0/24 para eficiencia.
- Enlaces punto a punto (/30) para optimizar la comunicación entre dispositivos clave.

### Red de Usuarios

- Rango de red principal: 172.16.0.0/16.
- Segmentado en máscaras de 24 bits para cada departamento, permitiendo flexibilidad y control.
- Facilita la gestión y aplicación de políticas de seguridad por segmento.



VLAN	Nombre VLAN	IP	Gateway	Descripción
10	Admisiones	172.16.1.0/24	172.16.1.1	Inscripciones y atención al público.
20	TI	172.16.2.0/24	172.16.2.1	Administración y gestión de red.
30	Seguridad	172.16.3.0/24	172.16.3.1	Monitorización y control de acceso.
40	RRHH	172.16.4.0/24	172.16.4.1	Gestión de recursos humanos.
50	Finanzas	172.16.5.0/24	172.16.5.1	Gestión financiera y contabilidad.
60	Biblioteca/Labs	172.16.6.0/24	172.16.6.1	Recursos académicos y laboratorios.
70	Recepción	172.16.7.0/24	172.16.7.1	Atención al visitante y comunicación.
80	Mantenimiento	172.16.8.0/24	172.16.8.1	Soporte técnico y mantenimiento de infraestructura.
100	Servidores	172.16.100.0/24	172.16.100.1	Servicios críticos (DHCP en 172.16.100.10).

Esta segmentación estratégica no solo facilita la organización, sino que también establece las bases para implementar políticas de seguridad y control de acceso más robustas, al permitir la aplicación de reglas específicas a cada segmento de red.

# Segmentación de VLANs del Campus JNA

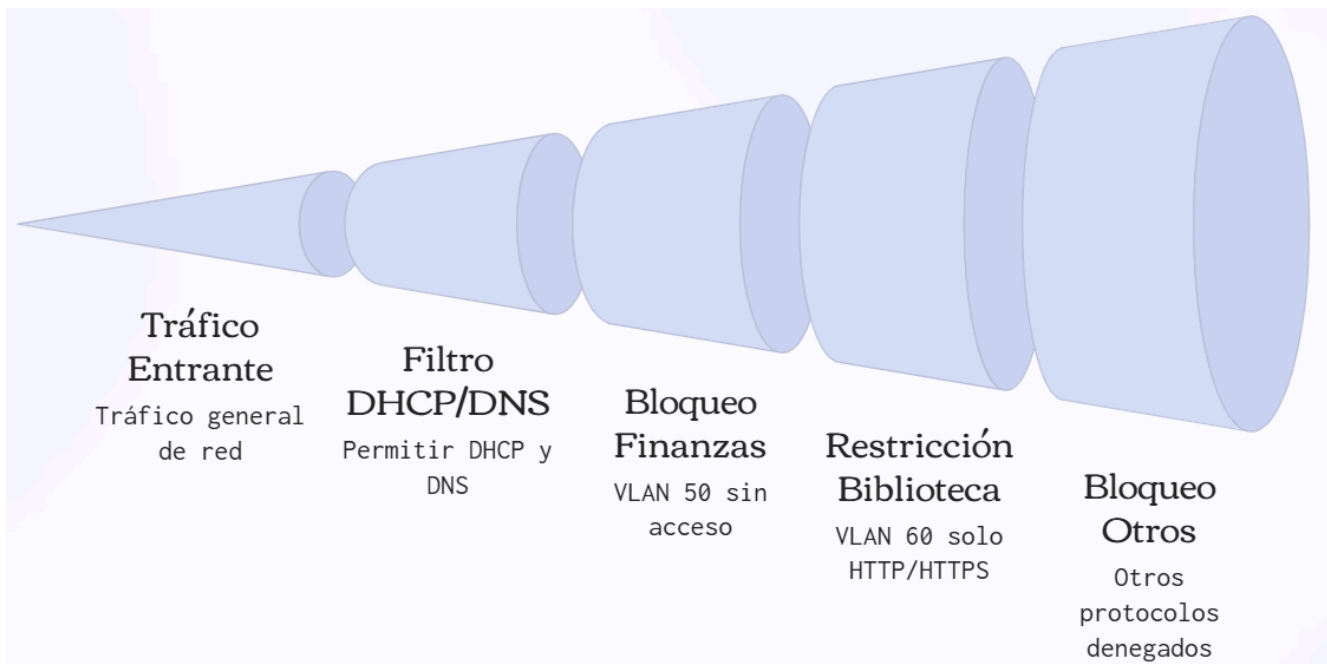
La segmentación de la red mediante VLANs es crucial para la seguridad, el rendimiento y la gestión del Campus JNA. Al dividir la red principal 172.16.0.0/16 en subredes /24 dedicadas para cada departamento y servicio, garantizamos un control granular del tráfico y la aplicación de políticas de seguridad específicas, optimizando los recursos de red y minimizando los riesgos.



Este esquema permite que cada departamento opere en su propio dominio de difusión, mejorando la eficiencia de la red y facilitando la resolución de problemas. Además, aísla el tráfico sensible, como el de servidores o finanzas, de otras áreas de la red, fortaleciendo la postura de seguridad general del campus.

## Diseño de Seguridad y Control de Acceso (ACL)

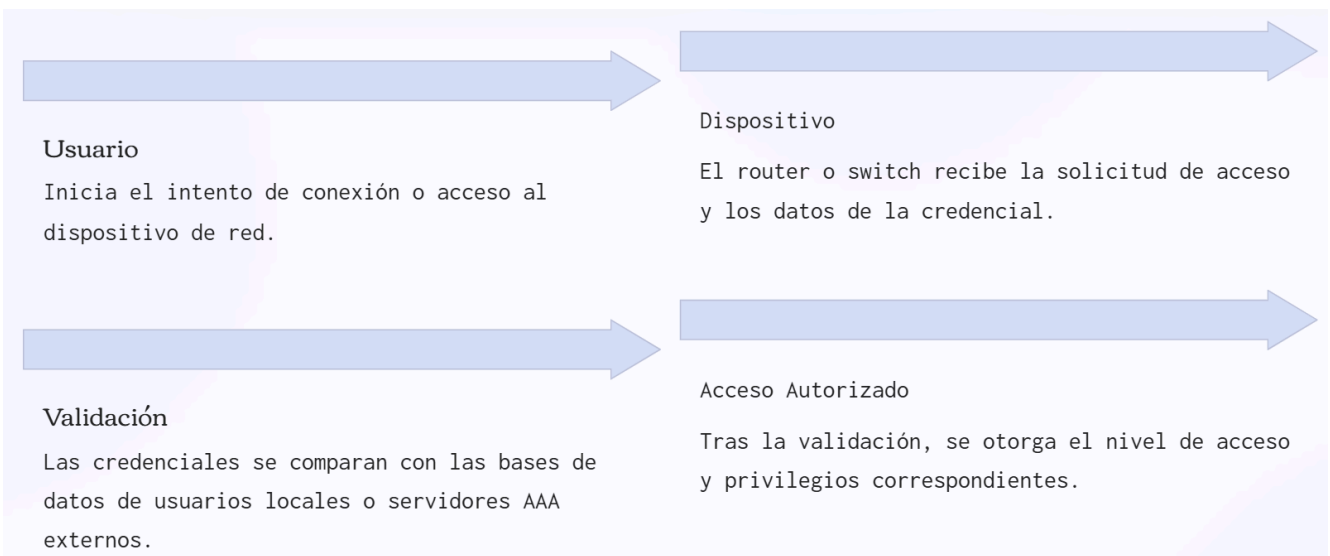
La seguridad de la información financiera y académica es una prioridad para el Campus JNA. Por ello, se ha implementado una política de seguridad granular mediante Listas de Control de Acceso (ACLs) extendidas, aplicadas en las interfaces SVI (Switch Virtual Interfaces) de los switches de distribución en dirección de entrada (inbound).



1	2	3
<b>Tráfico de Infraestructura Esencial</b> Se permite explícitamente el tráfico DHCP (BootPC/BootPS) y DNS hacia el servidor central (172.16.100.10) al inicio de cada ACL, asegurando el funcionamiento básico de la red antes de aplicar restricciones más estrictas.	<b>Aislamiento de Áreas Sensibles</b> VLANs como Finanzas (VLAN 50) y RRHH (VLAN 40) tienen prohibido el acceso a cualquier red interna no esencial ( <code>deny ip 172.16.0.0 255.255.0.0</code> ), aunque mantienen acceso a Internet, protegiendo así datos críticos.	<b>Restricciones para Usuarios (VLAN 60)</b> La VLAN de Biblioteca Digital/Laboratorios (VLAN 60) está estrictamente restringida a servicios web (puertos 80/443), evitando el uso de protocolos de transferencia de archivos no autorizados y manteniendo un ambiente seguro para el aprendizaje.

## Gestión de Identidades y Acceso (AAA)

Para asegurar la administración de los equipos de red, se ha implementado un esquema de Autenticación, Autorización y Contabilidad (AAA) que incluye niveles de privilegio diferenciados. Esto garantiza la trazabilidad de las acciones y minimiza el riesgo ante posibles compromisos de credenciales.



<b>Nivel de Privilegio: User</b> Acceso básico, solo para comandos de visualización y monitoreo.	<b>Nivel de Privilegio: Privileged</b> Acceso a comandos de configuración y funciones avanzadas, pero con restricciones.	<b>Nivel de Privilegio: Admin</b> Control total del dispositivo, incluyendo configuraciones críticas y sensibles.
<b>Acceso Local Único</b> Cada dispositivo (router, switch de distribución) cuenta con un usuario local único (ej. <code>rllocaluser</code> , <code>D1local</code> ). Esto permite una trazabilidad básica y facilita la identificación de la fuente de cualquier cambio o problema.	<b>Contraseñas Diferenciadas</b> Se utilizan contraseñas distintas para el modo de usuario y el modo privilegiado ( <code>enable</code> ). Esta práctica es fundamental para evitar el compromiso total de la red si una única contraseña es vulnerada, añadiendo una capa extra de seguridad.	<b>Trazabilidad Completa</b> La combinación de usuarios únicos y contraseñas segregadas asegura que cada acción administrativa pueda ser rastreada hasta su origen, facilitando auditorías y la resolución de problemas de seguridad.

# Credenciales Administrativas

Dispositivo	Tipo de Acceso	Nombre de Usuario	Contraseña / Secret
Rt1	Acceso Local (VTY/Console)	r1localuser	r1567
Rt1	Modo Privilegiado	---	r1local
Rt2	Acceso Local (VTY/Console)	r2LocalUser	r2678
Rt2	Modo Privilegiado	---	r2local678
DSW1	Acceso Local (VTY/Console)	D1Local	D1678
DSW1	Modo Privilegiado	---	d1local678
DSW2	Acceso Local (VTY/Console)	D2Local	D2678
DSW2	Modo Privilegiado	---	d2local678
DSW3	Acceso Local (VTY/Console)	D3Local	D3678
DSW3	Modo Privilegiado	---	d3local678



## Segmentación por VLANs: Organización del Tráfico

Para garantizar una gestión eficiente y una seguridad robusta, hemos segmentado el tráfico del campus en diversas VLANs, cada una con un propósito específico y políticas de acceso claras.

### Gestión Académica

- VLAN 10: Admisión
- VLAN 40: RRHH
- VLAN 50: Finanzas

### Recursos Estudiantiles

- VLAN 60: Biblioteca Digital
- VLAN 60: Laboratorios

### Servicios Técnicos

- VLAN 20: IT
- VLAN 80: Mantenimiento
- VLAN 100: Servidores

### Seguridad y Otros

- VLAN 30: Seguridad
- VLAN 70: Recepción



# Matriz de Conectividad y Verificación

El éxito de este proyecto fue validado a través de rigurosas pruebas de conectividad y verificación de servicios, asegurando que cada componente funcione según lo previsto.

## Pruebas de Conectividad

- **Ping/Traceroute:** Realizadas exhaustivamente para confirmar la conectividad extremo a extremo y la ruta de los paquetes.
- **Verificación DHCP:** Confirmación de la asignación dinámica de direcciones IP mediante el comando `show ip dhcp binding`.

## Validación de Servicios

- **Rutas EIGRP:** Validación de la tabla de enrutamiento con `show ip route eigrp` para asegurar la propagación correcta de las rutas.
- **Seguridad ACLs:** Confirmación del bloqueo de tráfico no autorizado entre VLAN 60 y VLAN 40 según la matriz de tráfico definida, demostrando la eficacia de las políticas de seguridad.

## Conclusión: Una Red Preparada para el Futuro

El diseño e implementación de la red del campus JNA representa un avance significativo en infraestructura tecnológica. Hemos establecido una red jerárquica, redundante y altamente segura, capaz de soportar las demandas académicas y administrativas de una universidad moderna. Esta solución no solo resuelve los desafíos actuales, sino que también sienta las bases para un crecimiento futuro sostenible y la integración de nuevas tecnologías.

Estamos convencidos de que esta infraestructura proporcionará una base sólida para la innovación y la excelencia educativa en la Universidad JNA.

