1

### 1. La Capa Colapsada: Distribución y Núcleo 🔄

En lugar de tener dispositivos separados para el Núcleo y la Distribución, una red pequeña generalmente combina estas funciones en un **único router potente** y uno o dos **switches principales** de Capa 3 o Capa 2 gestionables.

- **Dispositivos Clave:** El **router de borde (o firewall)** y el **Switch Central (o de Distribución/Núcleo)**.
- **Funciones Lógicas:**
    - **Conectividad a Internet:** Gestionada por el router, que aísla la red interna de la externa.
    - **Ruteo (Núcleo/Distribución):** Si la red usa **VLANs** (recomendado), el Switch Central gestionará el tráfico entre ellas (ruteo entre VLANs).
    - **Aplicación de Políticas (Distribución):** Aquí se configura la **Calidad de Servicio (QoS)** para dar prioridad al tráfico de voz y video.
    - **Seguridad:** El router/firewall aplica las ACLs y las políticas de seguridad de la red.

---

### 2. La Capa de Acceso 💻

Esta capa conecta directamente a los usuarios y sus dispositivos, y es la más importante para la **conectividad diaria**.

- **Dispositivos Clave: Switches de Capa 2** (el más común) y **Puntos de Acceso Inalámbrico (WAPs)**.
- **Funciones Lógicas:**
    - **Conexión Física:** Los cables de red de las paredes se conectan a estos switches.
    - **VLANs:** Los puertos del switch se asignan a las VLANs correspondientes (p. ej., el puerto 10 es para la VLAN de Datos, el puerto 11 es para la VLAN de Voz).
    - **Power over Ethernet (PoE):** Si se usan teléfonos IP o WAPs, los switches de Acceso deben soportar PoE para alimentarlos.
    - **Seguridad de Puerto:** Se limita el número de dispositivos que pueden conectarse a un puerto para prevenir el acceso no autorizado.

---

**3. Ejemplo Práctico de Flujo de Datos** 📊

Imaginemos un empleado haciendo una videollamada:

1. **Capa de Acceso:** El PC del empleado se conecta a un **Switch de Acceso** (Capa 2). El tráfico de videollamada se **etiqueta** (clasificación QoS) como tráfico de alta prioridad.
2. **Capa de Distribución/Núcleo Colapsada:** El tráfico se envía al **Switch Central**. Este switch:
    - Reconoce la etiqueta de alta prioridad gracias a la configuración de **QoS**.
    - Si necesita comunicarse con un servidor en otra VLAN, el Switch Central realiza el **ruteo entre VLANs**.
3. **Borde de Red:** El tráfico llega al **Router/Firewall**, que le da prioridad en la fila de espera para la **salida a Internet**, asegurando que el retraso (latencia) de la videollamada sea mínimo.

| Dispositivo Lógico/Función | Dispositivo Físico Común en una PyME |
|---|---|
| **Núcleo + Distribución** | Router/Firewall (con capacidad de ruteo) + Switch Central gestionable (L2/L3) |
| **Acceso** | Switches de Capa 2 (con PoE) + Puntos de Acceso Inalámbrico (WAPs) |

Este diseño colapsado ofrece **escalabilidad suficiente** para el crecimiento inicial y mantiene los **principios de seguridad y rendimiento** al segmentar el tráfico mediante VLANs y aplicar políticas de QoS en el Switch Central

**EJEMPLOS:**

**Fundamentos del Esquema de Direccionamiento IP con VLANs** 🔢

**1. Selección del Espacio de Direcciones** 🏠

Siempre se deben usar **direcciones IP privadas** para una red interna. Los rangos estándar son:

- **Clase A:** 10.0.0.0 a 10.255.255.255
- **Clase B:** 172.16.0.0 a 172.31.255.255
- **Clase C (el más común para PyMEs):** 192.168.0.0 a 192.168.255.255

**Recomendación para PyMEs:** Usaremos el rango **192.168.10.0/24** como base.

---

**2. Definición de Segmentos Lógicos (VLANs)** 👨‍💻

El primer paso es decidir cómo aislarás los grupos de dispositivos. La segmentación mejora la seguridad y el rendimiento al reducir el tráfico de difusión innecesario.

| VLAN ID | Propósito del Segmento | Dispositivos Incluidos |
|---|---|---|
| **VLAN 10** | **Datos de Empleados** | PCs, portátiles y teléfonos móviles personales. |
| **VLAN 20** | **Voz (VoIP)** | Teléfonos IP. (Se requiere su propio segmento para aplicar QoS). |
| **VLAN 30** | **Servidores y Gestión** | Servidor de archivos, impresora principal, dispositivos de red (switches, WAPs). |
| **VLAN 40** | **Invitados (Guest Wi-Fi)** | Dispositivos de visitantes. (Este segmento debe tener acceso a Internet **solamente**). |

¡Absolutamente! Diseñar un esquema de direccionamiento IP sólido es crucial. Una red pequeña no solo debe funcionar, sino que debe ser **segura**, **organizada** y **escalable**.

El fundamento clave aquí es usar la **segmentación (VLANs)** para dividir una única red física en múltiples redes lógicas (Subredes IP).

---

**Fundamentos del Esquema de Direccionamiento IP con VLANs** 🔢

**1. Selección del Espacio de Direcciones** 🏠

Siempre se deben usar **direcciones IP privadas** para una red interna. Los rangos estándar son:

- **Clase A:** 10.0.0.0 a 10.255.255.255
- **Clase B:** 172.16.0.0 a 172.31.255.255
- **Clase C (el más común para PyMEs):** 192.168.0.0 a 192.168.255.255

**Recomendación para PyMEs:** Usaremos el rango **192.168.10.0/24** como base.

---

### 2. Definición de Segmentos Lógicos (VLANs) 👨‍💻

El primer paso es decidir cómo aislarás los grupos de dispositivos. La segmentación mejora la seguridad y el rendimiento al reducir el tráfico de difusión innecesario.

| VLAN ID | Propósito del Segmento | Dispositivos Incluidos |
|---|---|---|
| **VLAN 10** | **Datos de Empleados** | PCs, portátiles y teléfonos móviles personales. |
| **VLAN 20** | **Voz (VoIP)** | Teléfonos IP. (Se requiere su propio segmento para aplicar QoS). |
| **VLAN 30** | **Servidores y Gestión** | Servidor de archivos, impresora principal, dispositivos de red (switches, WAPs). |
| **VLAN 40** | **Invitados (Guest Wi-Fi)** | Dispositivos de visitantes. (Este segmento debe tener acceso a Internet **solamente**). |

---

### 3. Asignación de Subredes IP (Subnetting) ➗

A cada VLAN se le asigna un segmento de la dirección IP base (Subred). Para optimizar el uso de direcciones, podemos usar la técnica de **subnetting** (dividir la red /24 en partes más pequeñas), adaptando el tamaño al número de hosts esperados.

Aquí se muestra un ejemplo de cómo dividir la red base **192.168.10.0/24**:

| Segmento | Subred IP / Máscara | Rango de Hosts (Aprox.) | Uso |
|---|---|---|---|
| **VLAN 30 (Servidores)** | **192.168.10.0/28** (Máscara: 255.255.255.240) | 14 hosts | **Direcciones IP Estáticas** (Predeterminadas). |
| **VLAN 10 (Datos)** | **192.168.10.16/26** (Máscara: 255.255.255.192) | 62 hosts | **DHCP** (Asignación dinámica). |
| **VLAN 20 (Voz)** | **192.168.10.80/26** (Máscara: 255.255.255.192) | 62 hosts | **DHCP** (Asignación dinámica). |
| **VLAN 40 (Invitados)** | **192.168.10.144/26** (Máscara: 255.255.255.192) | 62 hosts | **DHCP** (Asignación dinámica). |

**Nota sobre el Gateway:** El router o switch multicapa de Distribución tendrá una dirección IP en cada una de estas subredes (generalmente la primera dirección utilizable, como .1 o .17), y actuará como la **puerta de enlace (Gateway)** para todos los dispositivos de esa VLAN.

**. El Corazón del Diseño: Ruteo Entre VLANs (Inter-VLAN Routing)** 🧠

La clave de este diseño es que, aunque los segmentos están separados, la mayoría de ellos necesitan comunicarse entre sí (por ejemplo, los empleados necesitan acceder al servidor).

- **¿Quién Rutea?** El **Switch Central de Distribución** o un **Router dedicado** (si el diseño es más grande) debe tener la capacidad de **ruteo de Capa 3**.
- **Función:** Este dispositivo recibe el tráfico de una VLAN (por ejemplo, VLAN 10), consulta su tabla de ruteo y lo reenvía al segmento de destino (por ejemplo, VLAN 30), cruzando los límites de la subred.
- **Control:** Aquí es donde se implementan las **Listas de Control de Acceso (ACLs)** para hacer cumplir la seguridad. Por ejemplo: *Permitir que VLAN 10 acceda a VLAN 30*, pero *Denegar que VLAN 40 (Invitados) acceda a cualquier otra VLAN interna*.

| Tipo de Asignación | Dónde Usarla | Importancia |
|---|---|---|
| **Estática** | Dispositivos que deben ser predecibles: **servidores**, **impresoras de red**, **routers**, **switches**, **puntos de acceso** y otros equipos de infraestructura (VLAN 30). | Facilita la administración y la solución de problemas. |
| **Dinámica (DHCP)** | Dispositivos de usuario final: **PCs**, **portátiles**, **teléfonos IP** (VLANs 10, 20, 40). | Reduce la carga administrativa y evita errores manuales de IP. |

Este diseño crea una red segura, predecible y organizada que puede crecer con la oficina simplemente agregando más puertos de acceso y manteniendo el Switch Central como el punto de control.