**1.Realice una lista con al menos 3 ventajas y desventajas de adquirir un switch administrable en comparación con uno que no tenga dicha característica.**

**Ventajas de un switch administrable:**

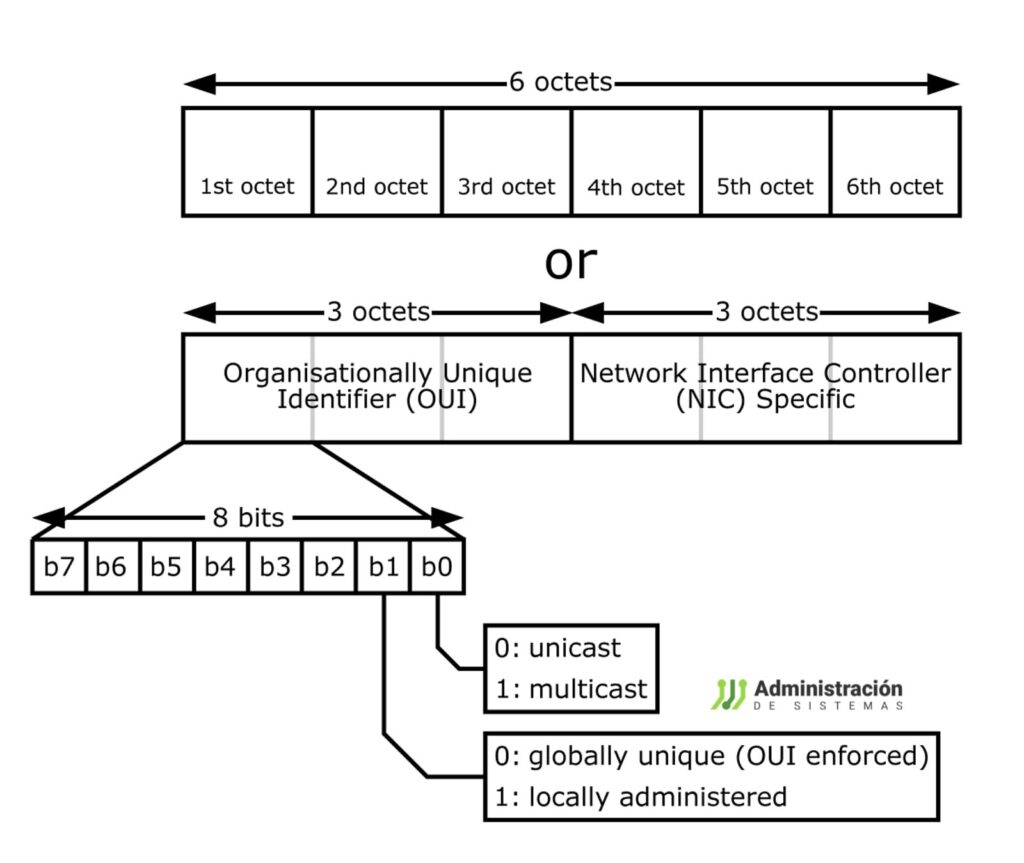
1. **Configuración avanzada**: permite gestionar VLANs, QoS (calidad de servicio), control de acceso y priorización de tráfico.
2. **Monitoreo y seguridad:** ofrece herramientas para detectar y prevenir ataques o problemas de red, como SNMP y port mirroring.
3. **Escalabilidad:** es más adaptable a redes complejas y crecientes, permitiendo configurar parámetros a medida que la red crece.

**Desventajas:**

1. **Costo elevado:** los switches administrables son más caros que los no administrables.
2. **Mayor complejidad:** requieren conocimientos especializados para configurarlos y administrarlos correctamente.
3. **Mantenimiento:** necesitan actualizaciones y gestión constante para asegurar su correcto funcionamiento.

**2. Investigue en qué consiste el ataque conocido como inundación de direcciones MAC (MAC Flooding Attack) y realice un diagrama donde se muestre su funcionamiento.**

El ataque de MAC Flooding funciona saturando la tabla CAM (Content Addressable Memory) de un switch con múltiples direcciones MAC falsas. Cuando la tabla se llena, el switch no puede asociar las direcciones MAC con los puertos correctos y empieza a comportarse como un HUB, reenviando el tráfico a todos los puertos. Esto permite que un atacante capture tráfico destinado a otros dispositivos.



**3. ¿Cómo se puede utilizar el ataque de inundación de direcciones MAC para hacer que un switch se comporte como HUB y realizar una escucha de todo el tráfico de los nodos conectados?**

El ataque de MAC Flooding provoca que el switch pierda su capacidad de enviar paquetes de manera selectiva, ya que su tabla de direcciones MAC está llena de entradas falsas. El switch envía todo el tráfico a todos los puertos, similar a un hub, permitiendo a un atacante usar herramientas de captura de tráfico (como Wireshark) para escuchar todo el tráfico de la red.

**4. Investigue la sintaxis del comando port security para un switch Cisco.**

*switchport port-security*

Otras opciones adicionales:

*switchport port-security maximum <cantidad> # Limita el número de direcciones MAC permitidas*

*switchport port-security violation <mode> # Define la acción cuando se detecta una violación*

*switchport port-security mac-address sticky # Activa el aprendizaje dinámico de MAC*

**5. Investigue qué permite realizar la opción sticky de port security.**

Permite que el switch aprenda dinámicamente las direcciones MAC conectadas a un puerto y las almacene como direcciones seguras. Estas direcciones quedan asociadas al puerto de forma dinámica, pero se pueden guardar en la configuración para su persistencia tras reinicios.

**6. Investigue cómo se podría utilizar la opción sticky de port security como una opción más flexible a MACs fijas.**

La opción **sticky** es más flexible que las MAC fijas porque, en lugar de tener que introducir manualmente las direcciones MAC, el switch las aprende automáticamente a medida que los dispositivos se conectan. Esto facilita la administración, ya que permite adaptarse a cambios sin intervención manual, pero mantiene seguridad similar a las MACs fijas.

**7. ¿Para qué se utiliza la opción aging de port security?**

La opción **aging** de port security permite definir cuánto tiempo una dirección MAC aprendida permanece activa en la tabla de seguridad antes de ser eliminada. Esto es útil para liberar espacio en la tabla y asegurar que las direcciones antiguas o dispositivos que ya no están conectados no ocupen un lugar innecesario en la configuración del puerto.