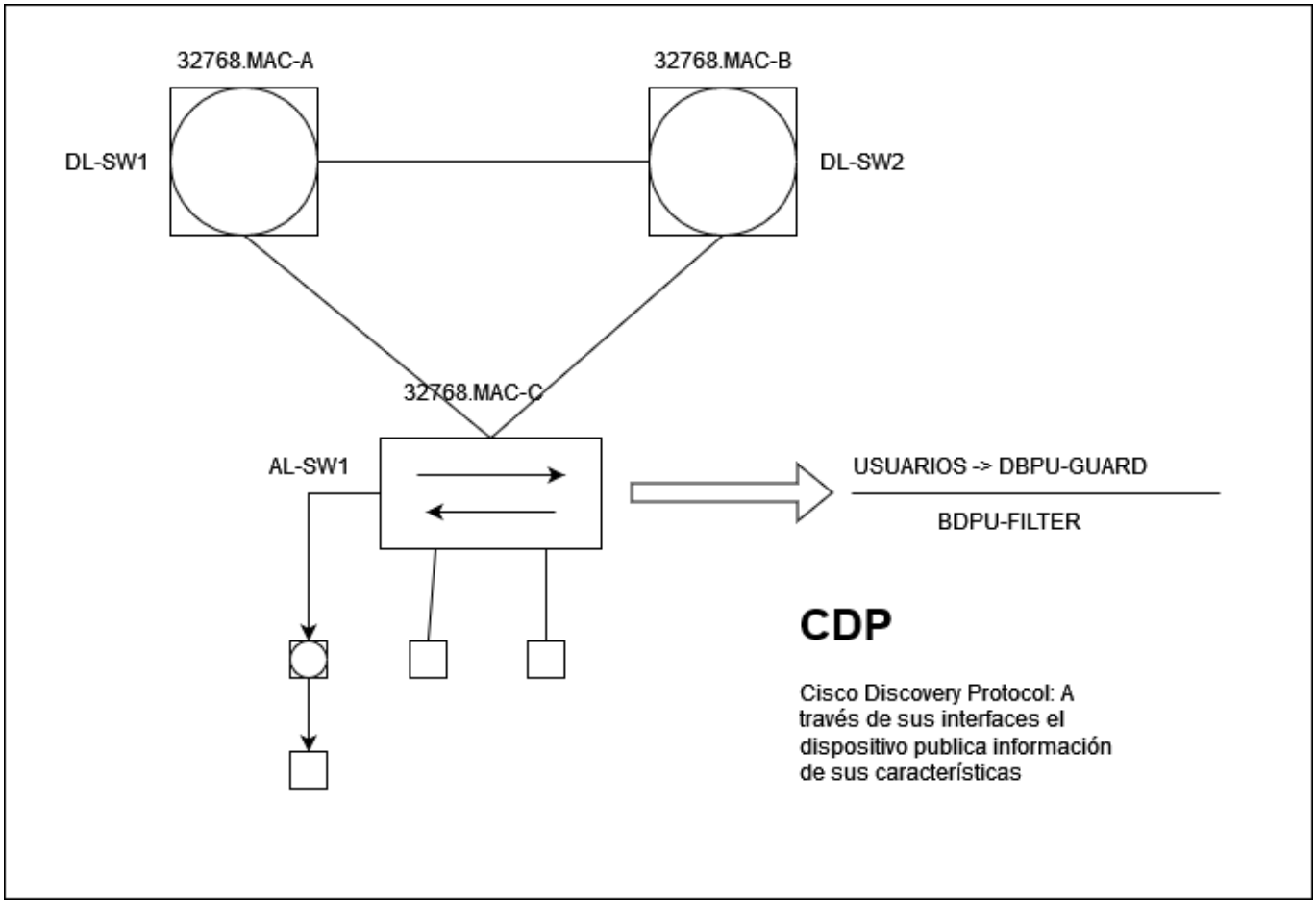
Seguridad LAN en entornos Ethernet

Configuridad de seguridad básica en Switches

- Contraseñas Seguras
  - Se debe usar siempre la opción secret, además de letras números y caracteres especiales.
  - Activar “service password-encryption” para evitar que las contraseñas se puedan descubrir mirando la configuración.
  - Utilizar gestión de usuarios AAA:
- Configuración de advertencias: Propósito disuasivo
  - “banner motd” o “banner login” como mensaje previo a la autenticación
  - Tanto para fines legales como administrativos, se configura un mensaje de advertencia.
- Acceso seguro a la consola: seguridad física y lógica configurando el control de acceso
- Acceso Seguro a través de líneas VTY:
  - Usar SSH2 en vez de telnet
  - Aplicar ACLs a las líneas VTY para limetar el acceso a solo las estaciones de gestión desde ciertas subredes. Se limita el acceso administrativo a determinadas IPs origen.
  - Uso de control de acceso AAA-NewModel
- Deshabilitar daemon HTTP:
  - Se recomienda su desactivación o, si no es posible, activar el modo HTTP secure con : “ip http secure-server”
  - Configurar ACLs para permitir acceso SOLO desde redes seguras.
- Deshabilitar servicios innecesarios
- Utilización de SNMPv3 con autenticaciín y privacidad y ACLs para limitar el acceso SNMP a las estaciones de trabajo y subredes de confianza

Asegurar topología de Spanning-Tree



- La introducción accidental o maliciosa de BPDUs puede bloquear un dispositivo o crear una denegación de servicio.
- Es necesario identificar al puente raiz configurando la prioridad
- Se debe activar la función “root-guard” para evitar que switches no autorizados se conviertan en raiz
- BDPU-Guard: Evita que los host envíen BPDUs de forma maliciosa de forma que si se recibe una BPDU maliciosa se desactiva el puerto hasta que sea reactivado por un administrador o hasta que pase cierta cantidad de tiempo.
- No se deben configurar BPDU guard y BPDU filter en el mismo puerto ya que podría generar bucles. Se reomienda que esté solo activa la funcionalidad BPDU filter
- Se debe reducir al mínimo el uso de CDP/LLDP.
- Configurar un sistema de log básico (Syslog)

Los switches Catalyst con Cisco IOS negocian automáticamente las capacidades de trunking:

	ACCESS	**Automatic**	**Desirable**	**Trunk**	**No Negotiate**
ACCESS	Acceso	Acceso	Acceso	ERROR	ERROR
Automatic	Acceso	Acceso	Trunk	Trunk	ERROR
Desirable	Acceso	Trunk	Trunk	Trunk	ERROR
Trunk	ERROR	Trunk	Trunk	Trunk	Trunk
No Negotiate	ERROR	ERROR	ERROR	Trunk	Trunk

- La negociación permite la introducción de un puerto de enlace troncal no autorizado en la red. Si uno de estos puertos no autorizados se usa para interceptar tráfico y generar ataques DDOS las consuecuencias pueden ser muchísismo peores que si se usa un puerto de acceso. Esto podría afectar a múltiples vlans.

- para evitar esto se desactiva la negociación automática de trunking en los puertos de acceso y en los troncales, además se eliminan las vlans no utilizadas en los troncales con “trunk allowed”

Para configurar esto existen los siguientes comandos:

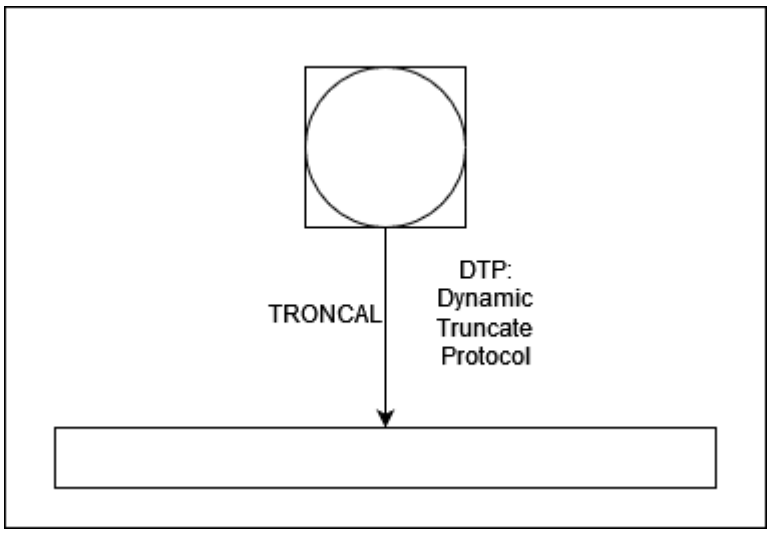
```
switchport mode trunk
switchport mode nonegotiate
switchport trunk vlan allowed
```

Configuración de puertos no utilizados:

- “shutdown”
- Colocarlos en una VLAN que no se propague por puertos trunking o en una vlan que no exista
- Definirlos como puetos de acceso, desacviando la negociación automática de trunking

Elaces troncales:

- Configurar manualmente todas las acciones trunk y deshabiltiar DTP
- Configurar una VLAN nativa (VLAN sin etiqueta) que solo esté operativa en los enlaces troncales.
- Una VLAN nativa es una propiedad e los enlaces troncales que asigna una vlan sin etiqueta, lo normal es que estas no se utilicen, en switches modernos pueden ser deshabilitadas.



La VLAN 1 siempre está habilitada, el tráfico de servicio va por la VLAN 1, aunque se trate de deshabilitar el switch no va a obedecer.

From:
https://knoppia.net/ - **Knoppia**

Permanent link:
https://knoppia.net/doku.php?id=redes:segether&rev=1729267657

Last update: **2024/10/18 16:07**