

# Instituto Tecnológico de las Américas



**Nombre:** Emmanuel Bello Sierra

**Matricula:** 2024-1369

**Profesor:** Jonathan Rondon

**Asignatura:** Seguridad de Redes

**Tema:** Tarea Semana 4 (Practica 3) P3

**Fecha:** 13 / 2 / 2026

## 1. Descripción y Objetivo del Script

Este proyecto demuestra un ataque al protocolo **Spanning Tree Protocol (STP)**. El objetivo es forzar una re-convergencia de la topología de red de Capa 2 para que la máquina atacante sea elegida como el **Root Bridge** (Punto Raíz).

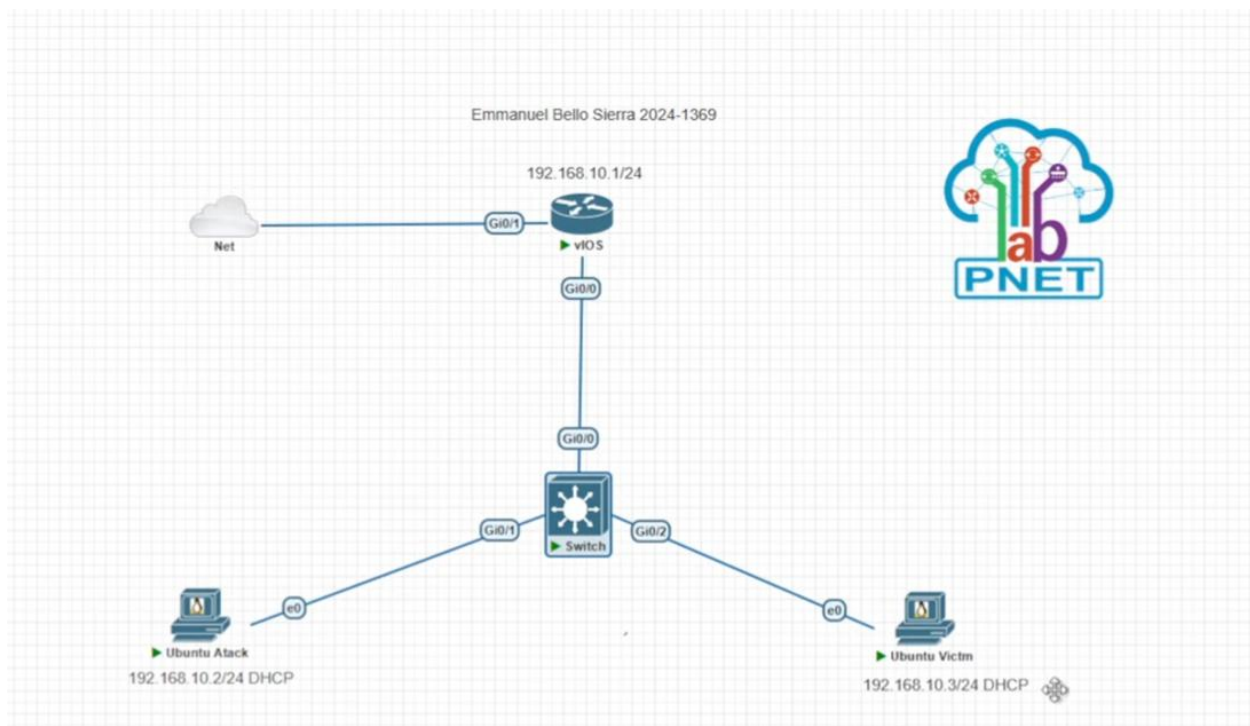
El script inyecta paquetes BPDU (Bridge Protocol Data Units) falsificados, anunciando una **Prioridad de Puente de 0** (la mejor posible) y un costo de ruta de 0. Dado que los switches Cisco por defecto tienen una prioridad de 32768, el switch legítimo cede su rol de Root, permitiendo al atacante atraer tráfico y controlar la topología.

## 2. Topología de Red

Switch Víctima: Cisco IOS (Prioridad 32768).

Atacante: Ubuntu con Scapy (Anuncia Prioridad 0).

Enlace: Conexión troncal o de acceso en la interfaz `ens3`.



### 3. Requisitos para Ejecutar

Python 3 + Scapy.

Acceso a la red física (o virtual en PNETLab).

Permisos de Root.

### 4. Parámetros Utilizados

Interfaz: `ens3`

Root ID (Priority): `0` (Superior a 32768).

Bridge ID: `0`

Path Cost: `0`

BPDU Type: Configuration BPDU (0x00).

### 5. Evidencia de Funcionamiento

Estado Original (Root es Cisco)

```
Switch#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    32769
             Address     5041.7d00.0300
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
             Address     5041.7d00.0300
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface                Role Sts Cost      Prio.Nbr Type
-----
Gi0/0                    Desg FWD 4         128.1   Shr
Gi0/1                    Desg FWD 4         128.2   Shr
Gi0/2                    Desg FWD 4         128.3   Shr
Gi0/3                    Desg FWD 4         128.4   Shr
Gi1/0                    Desg FWD 4         128.5   Shr
Gi1/1                    Desg FWD 4         128.6   Shr
Gi1/2                    Desg FWD 4         128.7   Shr
Gi1/3                    Desg FWD 4         128.8   Shr
--More--
```

## Resultado (Root es el Atacante)

```
Switch#
Switch#sh spanning-tree

VLAN0001
  Spanning tree enabled protocol rstp
    Root ID    Priority    0
              Address    502e.be00.0500
              Cost        4
              Port        2 (GigabitEthernet0/1)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

    Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
              Address    5041.7d00.0300
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time   300 sec

Interface      Role Sts Cost      Prio.Nbr Type
-----
Gi0/0          Desg FWD 4         128.1   Shr
Gi0/1          Root FWD 4         128.2   Shr Peer(STP)
Gi0/2          Desg FWD 4         128.3   Shr
Gi0/3          Desg FWD 4         128.4   Shr
Gi1/0          Desg FWD 4         128.5   Shr
Gi1/1          Desg FWD 4         128.6   Shr
Gi1/2          Desg FWD 4         128.7   Shr
--More--
```

## 6. Video Demostrativo

Explicación detallada y demostración del cambio de topología:

👉 [https://www.youtube.com/watch?v=eUiK5xAz\\_TM](https://www.youtube.com/watch?v=eUiK5xAz_TM)

## 7. Medidas de Mitigación

Para evitar que dispositivos no autorizados alteren la topología STP, se deben implementar Root Guard y BPDU Guard.

Configuración en Cisco IOS:

! En puertos de acceso de usuarios finales

```
Switch(config)# interface Gi0/1
```

```
Switch(config-if)# spanning-tree bpduguard enable
```

! Si se recibe un BPDU, el puerto se apaga.

! En puertos donde podría conectarse otro switch pero no debe ser Root

```
Switch(config)# interface Gi0/2
```

```
Switch(config-if)# spanning-tree guard root
```