HACKING ÉTICO: MANIPULANDO O SPANNING-TREE COM KALI LINUX E SCAPY

INSTITUTO FEDERAL
Goiás
Câmpus Formosa

SECITEC
SEMANA DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA

Prof. Mario Lemes

07/12/2021 (09:00 às 10:00)

AVISO DE ISENÇÃO

- Todos os conteúdos, atividades e aplicações (softwares) mostrados nesta conferência possuem objetivos 100% educativos, no qual o palestrante e o IFG não possuem qualquer responsabilidade em relação ao mal uso que os participantes possam fazer com as informações adquiridas.

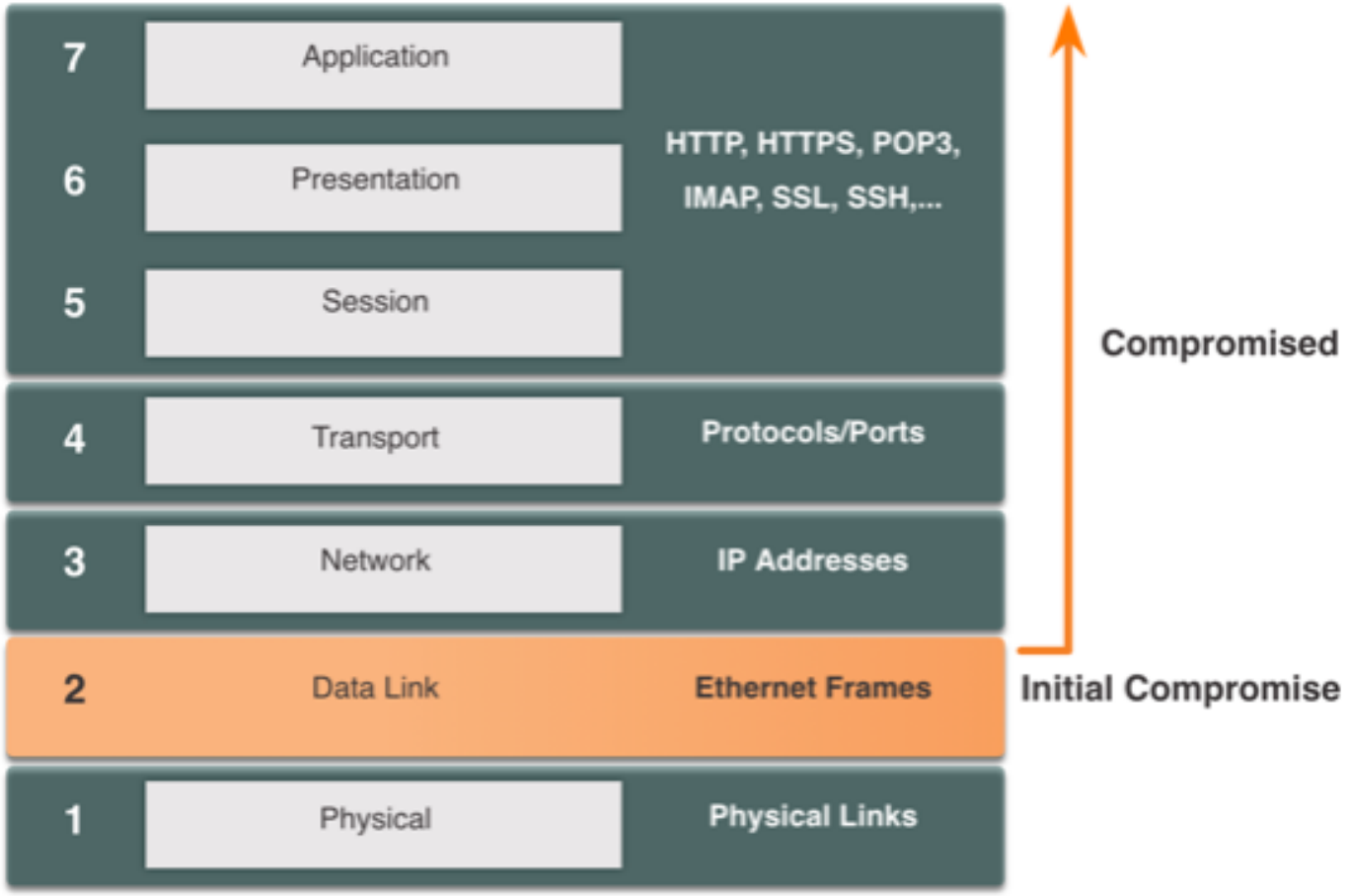
- O hacking ético é feito pelo "hacker do bem". Este é um profissional de TI com alta especialização em invasão de sistemas e detecção de vulnerabilidades, que se passa por um invasor e faz ataques programados para tentar achar brechas de invasão de um sistema.

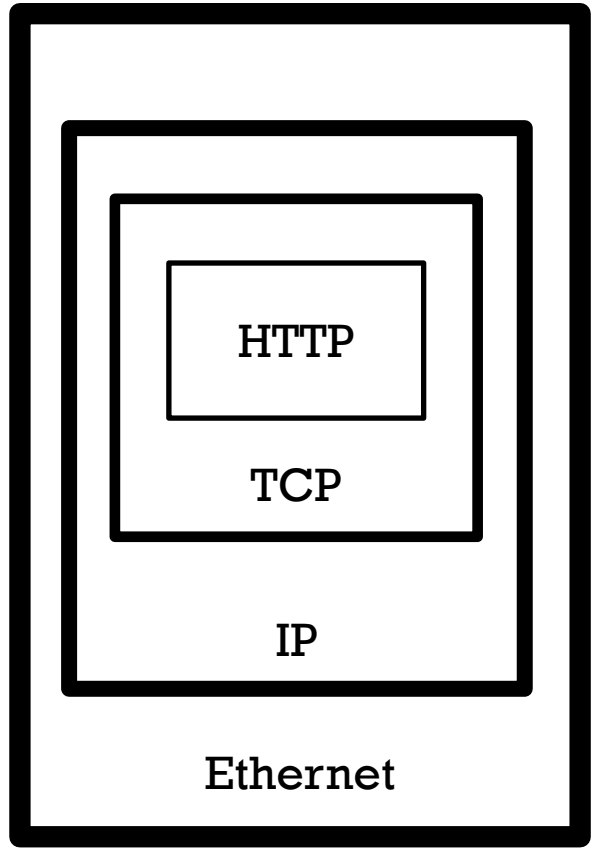
- Não use as informações deste seminário para hackear redes/sistemas que você não tem permissão.

SOBRE O PROFESSOR

- Mestre em Ciência da Computação.
- Especialista em Sistemas de Informação.
- Bacharel em Engenharia de Computação.
- Instrutor CCNA (Cisco Certified Network Associate) pela academia Cisco IFG – Campus Formosa.
- Certificado pela Huawei Certified ICT Associate 5G e fundador da Academia Huawei no IFG – Campus Formosa.
- Professor e pesquisador do IFG Campus Formosa com atuação nas seguintes áreas: Redes de Computadores, Sistemas Distribuídos, Segurança da Informação, Telecomunicações, Software/Hardware livre e Internet das Coisas.

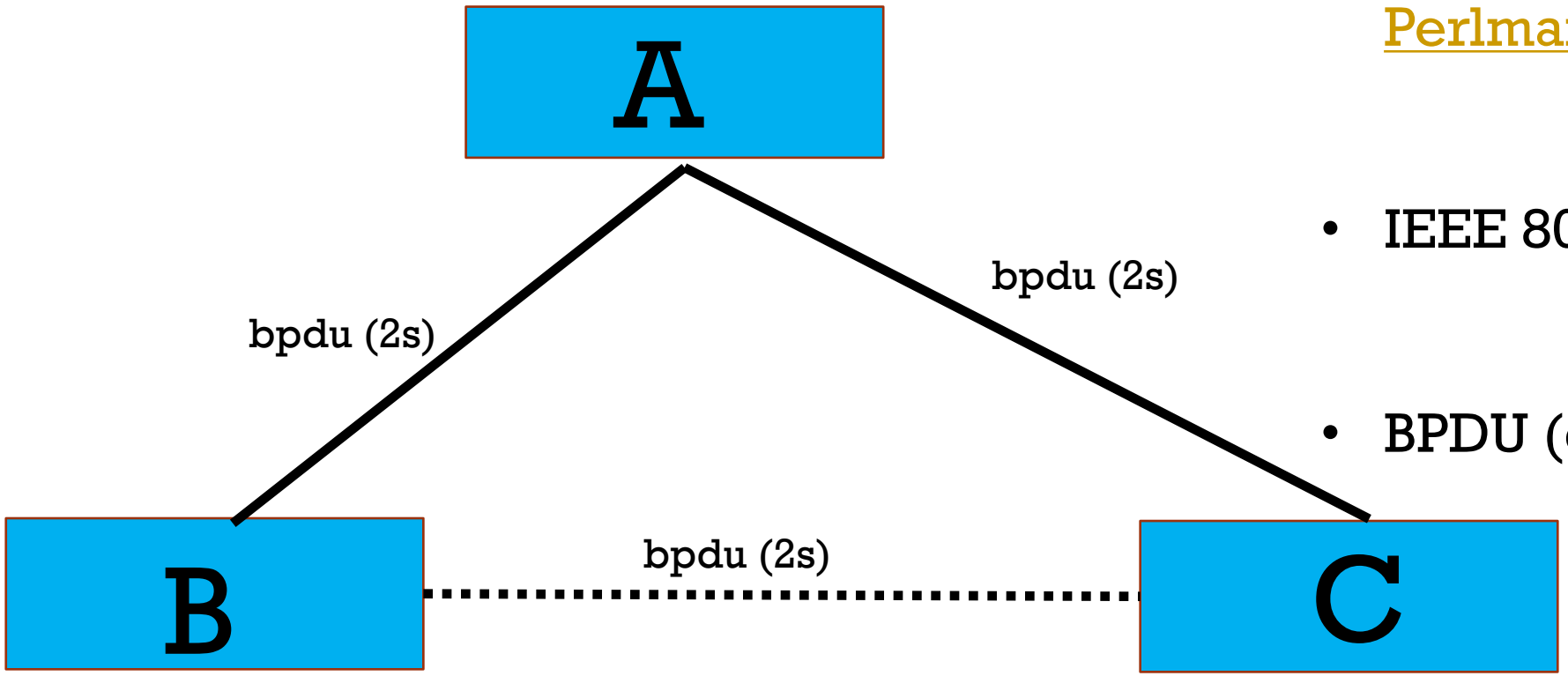
POR QUE SEGURANÇA DA CAMADA L2?





OBJETIVO DO SPANNING-TREE (SPT)

- **Objetivo**: Permitir o uso de links redundantes em redes de computadores sem que haja loop.



- Criado por Radia Perlman;
- IEEE 802.1D (STP);
- BPDU (default: 2s);

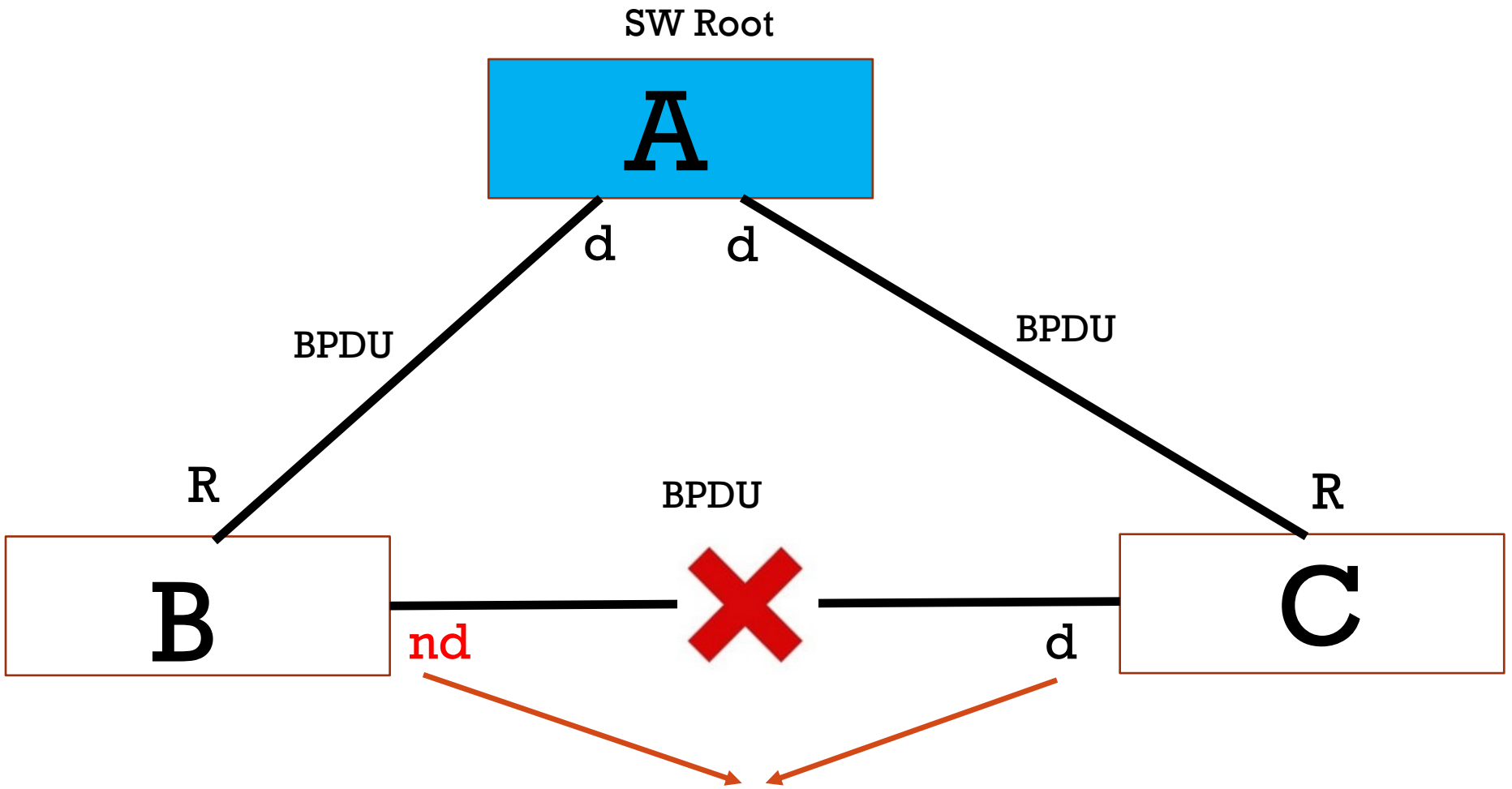
CONCEITOS DO SPT

- **Switch Role:**
  - Root (Todo tráfego da rede necessariamente passa pelo Switch Root).
  - Non-Root.

- **Port Role:**
  - Root (Enviar (para) ou receber (de) tráfego do Switch Root).
  - Designated (Deverá estar designada a assumir o papel de uma porta root caso a mesma falhe).
  - Non-Designated

- **Considerações importantes:**
  - Só existe um Switch Root.
  - Switch Root não tem porta root.
  - Só existe uma porta root nos SWs Non-Root.

OPERAÇÃO DO SPT



Um dessas duas portas deve se tornar Não-Designada/Alternativa

OPERAÇÃO DO SPT

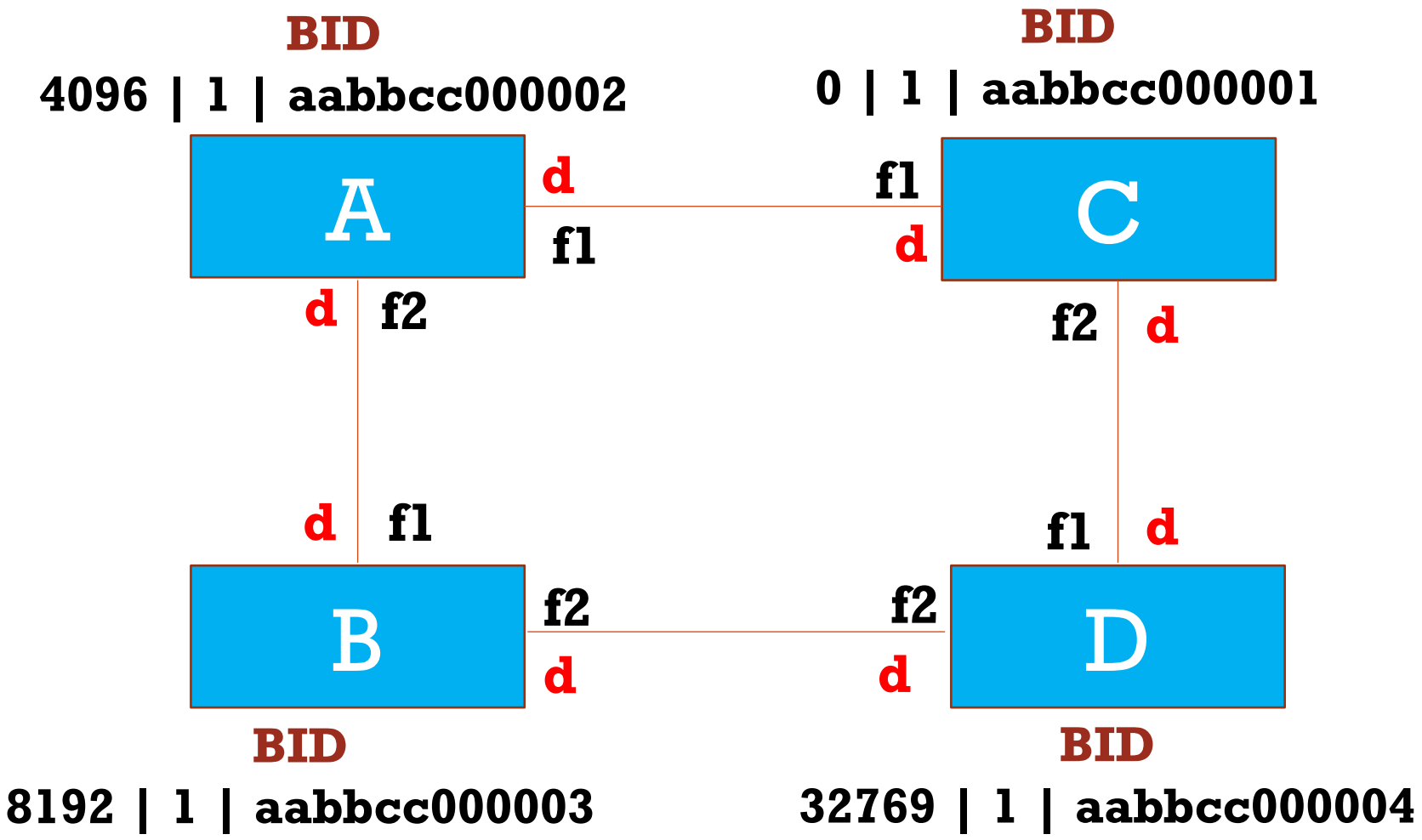
- **Switch Role:**
  - Root - Todo tráfego da rede necessariamente passa pelo Switch Root.
  - Non-Root.

- **Port Role:**
  - Root - Enviar (para) ou receber (de) tráfego do Switch Root.
  - Designated (Deverá estar designada a assumir o papel de uma porta root caso a mesma falhe).
  - Non-Designated - Portas vizinhas que sejam designadas devem se tornar não designadas (uma delas)

- **Port Status:**
  - **Blocking** - A porta Não-Designada deve assumir este estado
  - **Listening** } Estados transitórios
  - **Learning**
  - **Forwarding** - Portas Root e Designadas devem assumir este estado.
  - **Disabled** - Porta desabilitada.

30 seg

COMO FUNCIONA O SPT?



1° Quem será o SW Raiz?

2° Quem serão as portas Raiz de cada SW não raiz? Qual estado inicial das portas?

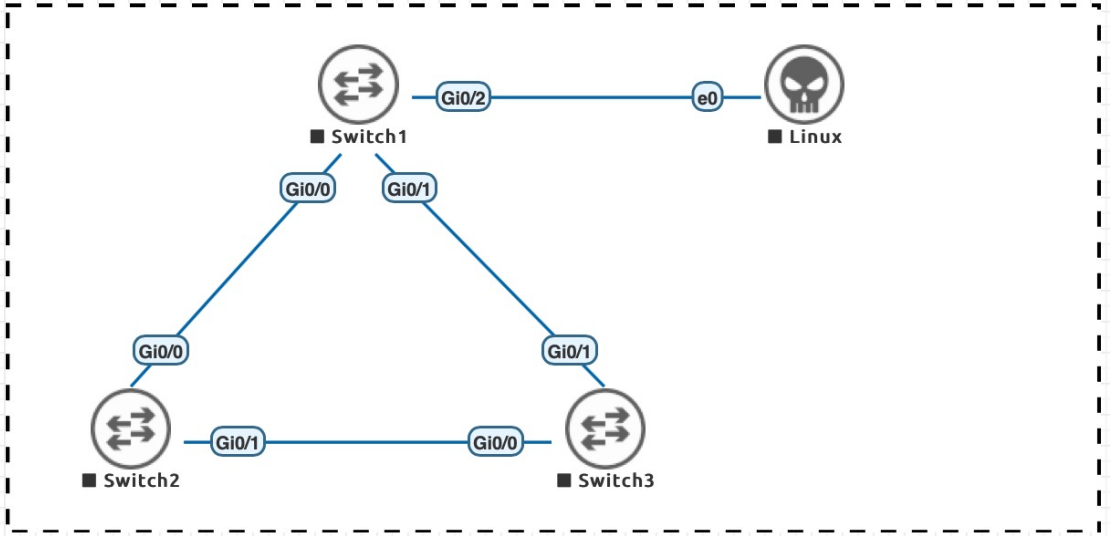
3° Quem serão as portas designadas e as portas não-Designadas?

Blocking – Listening – Learning - Forwarding - Disabled

VAMOS PARA PRÁTICA?

Emulated Virtual Environment
Next Generation

Hacking Ético: Manipulando o Spanning-Tree



Prof. Mario Lemes (IFG-Campus Formosa)

CONTRA-MEDIDAS AO ATAQUE DE MANIPULAÇÃO AO SPT

- Portas de acesso (conectam o switch a um host) não são confiáveis.

- Deve-se aplicar nas portas de acesso as seguintes medidas de segurança:

  - **BPDU guard**: imediatamente **desativa** uma porta que recebe uma BPDU.

  - **PortFast**: porta de acesso sai do estado "blocking" e vai direto para o estado "forwarding", ignorando estados transitórios ("listening" e "learning").

DÚVIDAS?

QUESTIONAMENTOS?

COMENTÁRIOS?

OBRIGADO PELA PARTICIPAÇÃO!

- Prof. Mario Lemes (IFG – Campus Formosa)

- Contato: mario.lemes@ifg.edu.br
- Currículo lattes: http://lattes.cnpq.br/4918126641251231
- Site pessoal: https://mariotlemes.github.io
- Youtube: http://www.youtube.com/c/MarioTeixeiraLemes?sub_confirmation=1
- Slides: https://url.gratis/TJwPnj