Segurança Cibernética

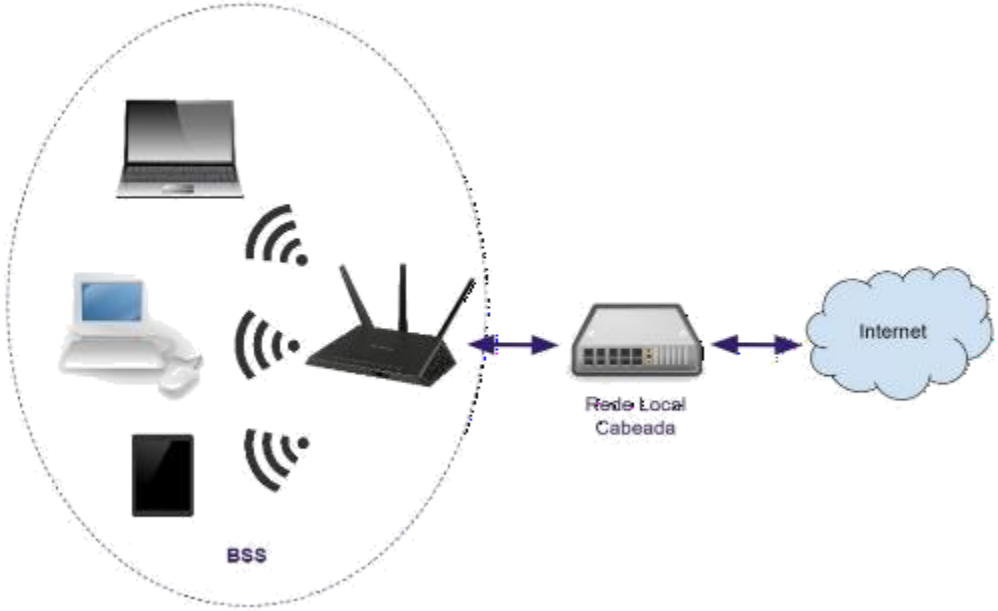
Ameaças, Vulnerabilidades e Ataques III:
Segurança em Redes Sem Fio

Prof. Dr. Daniel Caetano

2022 - 1

Compreendendo o problema

- **Situação:** A busca por conforto nos faz queremos nos livrar dos fios. Atualmente podemos interconectar uma grande quantidade de dispositivos com esse tipo de rede.



Mentimeter

Quais elementos compõem uma rede "wifi"?

Compreendendo o problema

- **Situação:** Essa liberdade, como qualquer outra, tem seu preço. Sem os fios para guiá-los, os dados são espalhados pelos ambientes, podendo ser coletados por qualquer equipamento.

Mentimeter

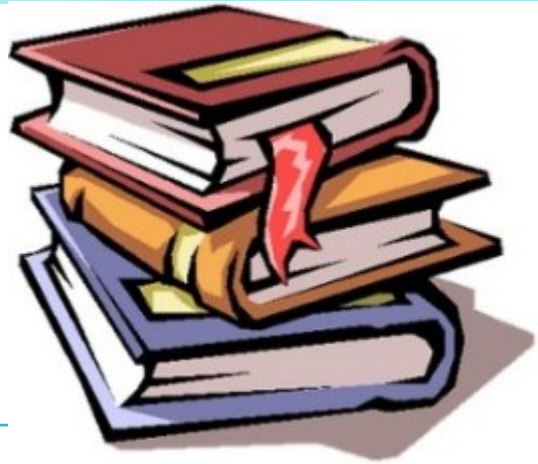
Quais são os mecanismos de proteção em redes wifi?

Objetivos

- Conhecer os elementos básicos das redes sem fio
- Conhecer os principais ataques
- Compreender os tipos de ataques e os mecanismos básicos de proteção
- Compreender os princípios de configuração de redes sem fio

- **Atividade Avaliativa A!**
  - **Conteúdo digital nas próximas a**

Material de Estudo



Material	Acesso ao Material
Notas de Aula e Apresentação	https://www.caetano.eng.br/aulas/2022a/ara0076.php (Segurança Cibernética – Aula 06)
Minha Biblioteca	• Segurança em Redes sem Fio: Guia do Iniciante (ISBN: 978-0-07-178028-5), págs 18, 81 e 107. • Segurança de Computadores: Princípios e Práticas (ISBN: 978-85-352-6449-4), págs 669.
Material Adicional	1) Usando o Roteador WiFi no Packet Tracer – Parte 1 – Dispoinível em: https://youtu.be/6BvpG_aWE50 (ative legenda e a tradução!) 2) Usando o Roteador WiFi no Packet Tracer – Parte 2 – Dispoinível em: https://youtu.be/3fdy2sIbfaI 3) Quebrando o WiFi WAP2 Handshake – Disponível em: http://

Visão Geral:

As Redes Sem Fio do Tipo Wi-Fi (802.11)

Redes sem fio

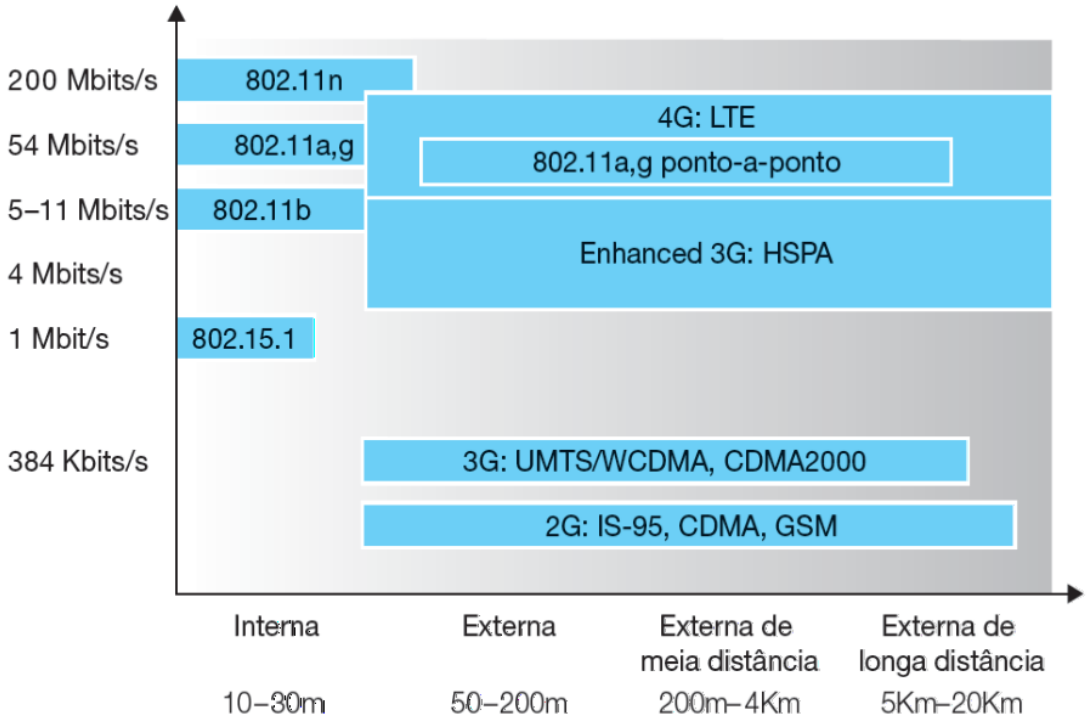
Bluetooth

- Propiciaram inúmeras inovações
  - Liberdade para os *Notebooks*
  - Celulares
  - Fones sem fio
  - IoT
  - ...

4G

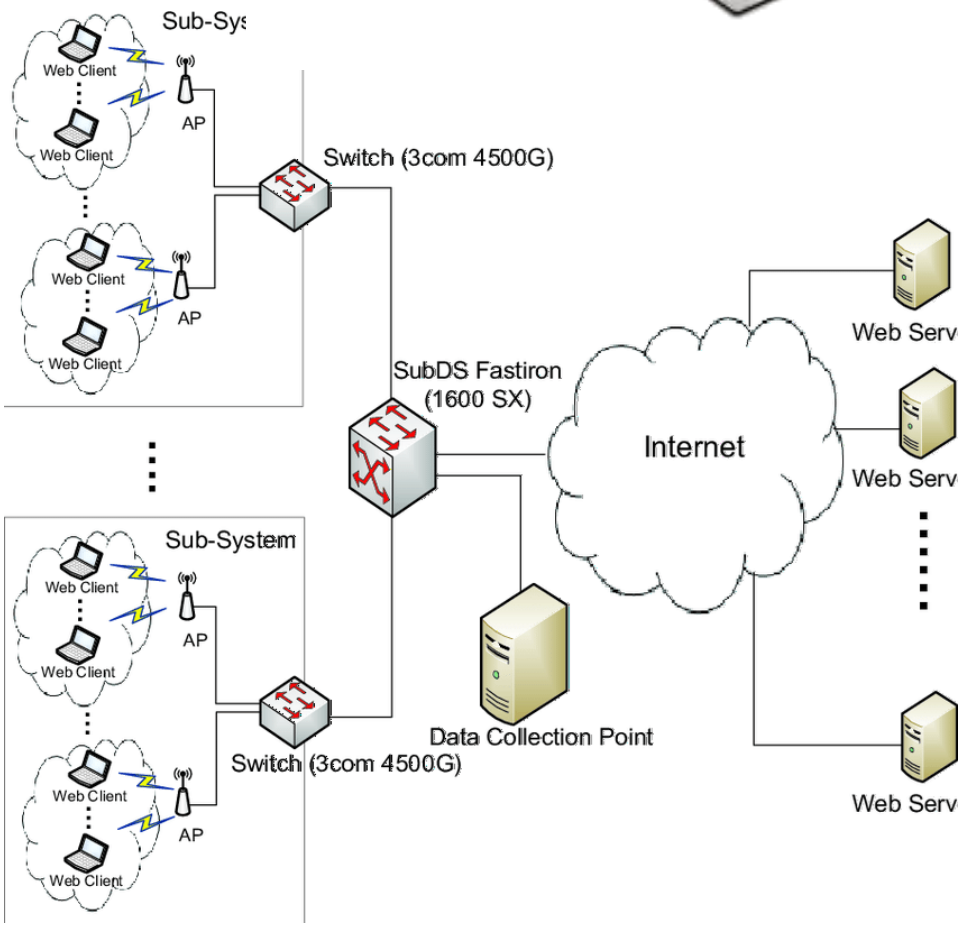
Wi-Fi

...



Redes sem fio

- Como funcionam?
  - *Ad-hoc*
  - Infraestrutura
    - Pontos de acesso sem fio
    - Interconectados por rede cabeada



Redes sem fio

- Equipamentos usuais:
  - *Access Point* (AP, ponto de acesso)
    - Apenas faz a conexão
  - Roteador *Wireless* (Roteador + AP)
    - Faz conexão e inclui recursos de roteamento
    - Em geral serve DHCP
  - “Estações” WiFi

Redes sem fio

- Configuração
  - Manual
    - Dados da conexão: SSID, canal, criptografia, chave...
  - WPS: *Wireless Protected Setup*
    - PIN (*Personal Information Number*)
      - Número de 8 dígitos
    - PBC (*Push Button Configuration*

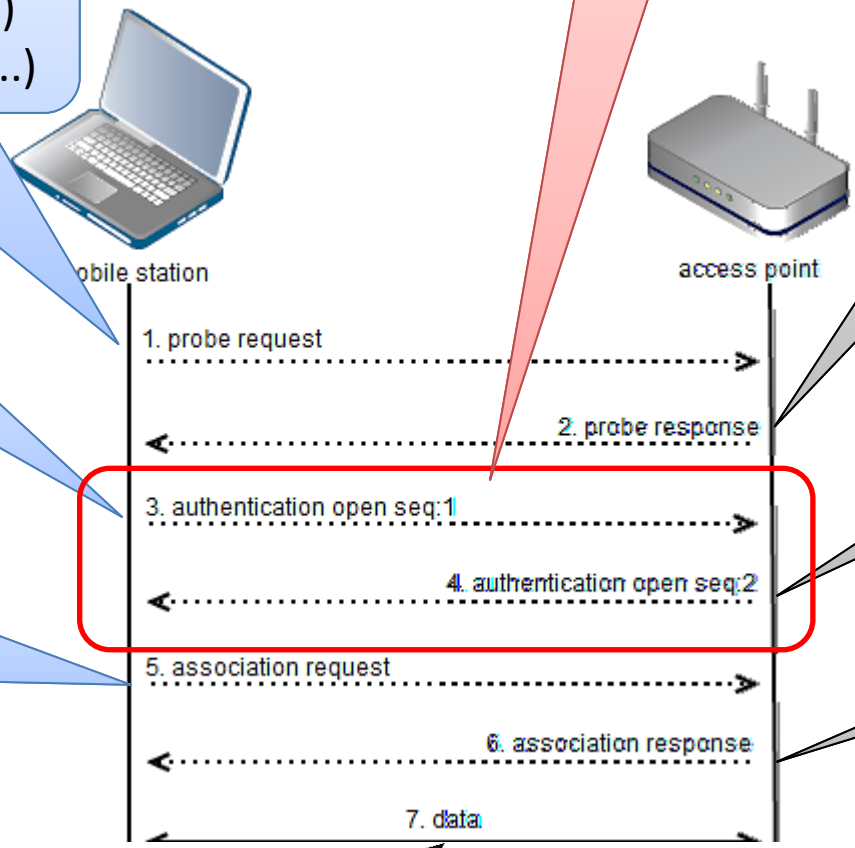
Conexão WiFi

- Processo de conexão

Pode ocorrer com vários APs

Espécie de *broadcast* (MAC FF:FF:FF:FF:FF:FF) nos formatos (b/g/n/ac...)

SSID e demais configurações



Requisição de Autenticação de Baixo Nível

Confirmação da Autenticação de Baixo Nível

Solicita Associação ao AP escolhido

Responde com ID de associação

Em uma rede aberta, inicia a troca de dados

Tipos de ataques comuns

- Usando adaptadores em “modo monitor”
  - Similar ao modo “promíscuo”
  - Ataques usuais:
    - Força Bruta no WPS (modo PIN)
    - Monitoramento de tráfego / Crack
    - Monitoramento de conteúdo (rede
    - DoS por desconexão.
- Usando APs portáteis (ou Tethe
  - Redes Abertas WiFi Falsas
  - Evil Twin (Gêmeo do mal – varia

PROTEGENDO A REDE WIFI

Como proteger a rede?

- Redes Abertas (sem criptografia)
  - Gerais de rede
    - Rede interna com IPs inválidos (para IPv4)
      - Uso de DMZ – DeMilitarized Zone
    - Filtrar pelo MAC Address .
  - Específicas WiFi
    - Esconder o SSID
    - Desligar o WPS.

Como proteger a rede?

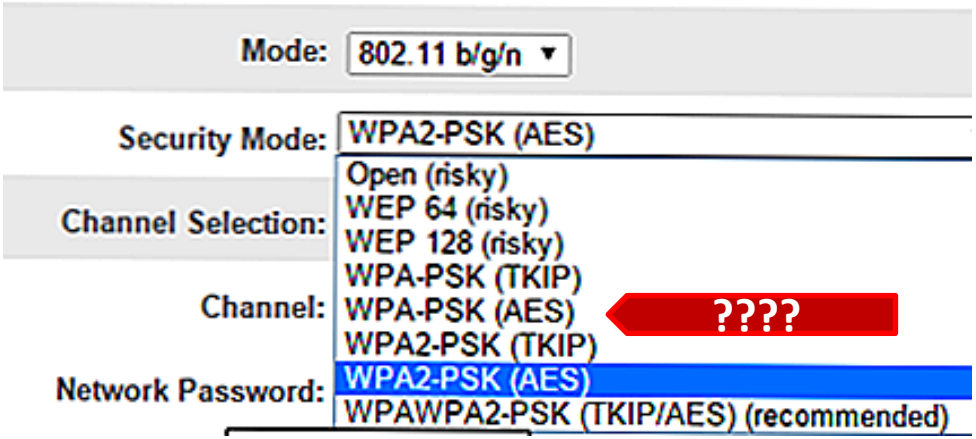
- Redes Criptografadas
  - IPs / Esconder o SSID / Filtrar MAC / Desligar WPS
  - Criptografia: vários protocolos
    - WEP – Wired Equivalent Privacy
    - WPA – WiFi Protected Access
      - EAP: Extensible Authentication Protocol
    - WPA2 – Evolução:
      - Personal: PSK – Pre-Shared Key
      - Enterprise: Servidor de autenticação
      - Falhas: https://www.techtudo.com.br/noticias/2017/10/falha-em-protocolo-wpa2-de-redes-wi-fi-provoca-corrida-por-solucao.ghtml

Como proteger a rede?

- Redes Criptografadas
  - Criptografia: vários protocolos
    - WPA3 – Já disponível em equipamentos novos
      - Criptografia de 192 bits (128 no modo personal)
        - » SAE: Simultaneous Autentication of Equals
          - Substitui o PSK
          - Criptografia individual para cada par de dispositivos.
          - “Dragonfly” handshake
      - Dificulta ataques de força bruta
      - Não permite DEAUTH a partir de dispositivos não autenticados
      - Falhas: https://www.tecmundo.com.br/seguranca/140318-senha-wifi-hackeada-via-falhas-protocolo-wpa3.htm

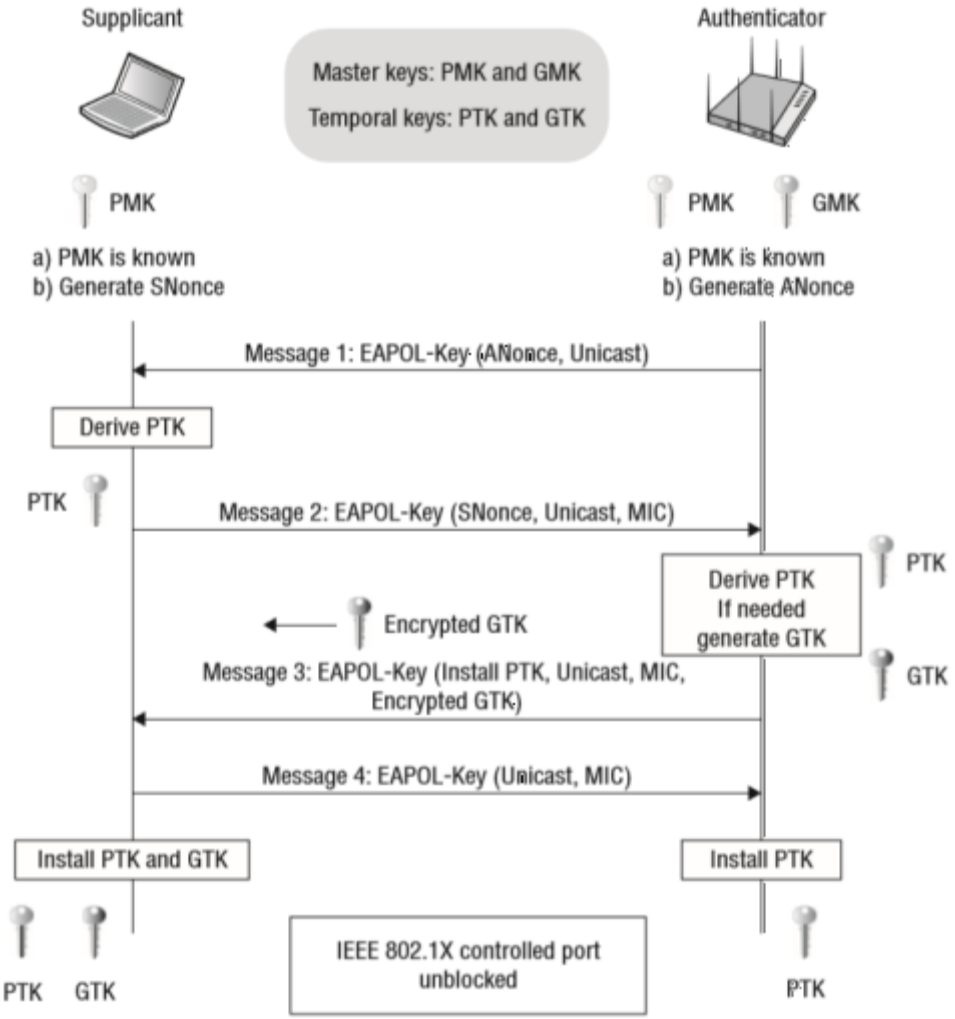
Criptografia WiFi - WPA/WPA2

- Protocolo: EAP
- Algoritmos?
  - WPA:
    - TKIP: Temporal Key Integrity Protocol
  - WPA2/WPA3:
    - TKIP: Temporal Key Integrity Protocol (compat.)
    - AES: Advanced Encryption Standard



WPA2 é 100% seguro?

- Não! **https://youtu.be/WfYxrLaqlN8**



Krack

Força Bruta

Deauth

WPA3 é 100% seguro?

- Nada é 100% seguro!
  - Mas falhas do WPA3 não justificam regressão
    - Falha “dragonblood”
      - Corrigida: “hash-to-element”
  - Eventuais falhas do WPA3 têm sido corrigidas
    - Até quando?
    - https://arxiv.org/pdf/2012.02745.pdf
    - WPA4...?

Dicas de proteção

- Redes abertas
  - Nunca confiem! Não usem com nada sério!
  - No mínimo, usem uma VPN!
- Desligue o WiFi quando não usar
  - Seus apps podem mandar dados sem você saber
- Não use Apps importantes em redes públicas
  - Logadas ou não... Nada de App Banking!

RECORDANDO:

PACKET TRACER CISCO

Inscrição no NetAcad

- Criar conta
  - https://www.netacad.com/pt-br
  - Entrar > Entrar
  - Registrar-se
  - Ativar a conta no seu e-mail

Inscrição no Curso e Download

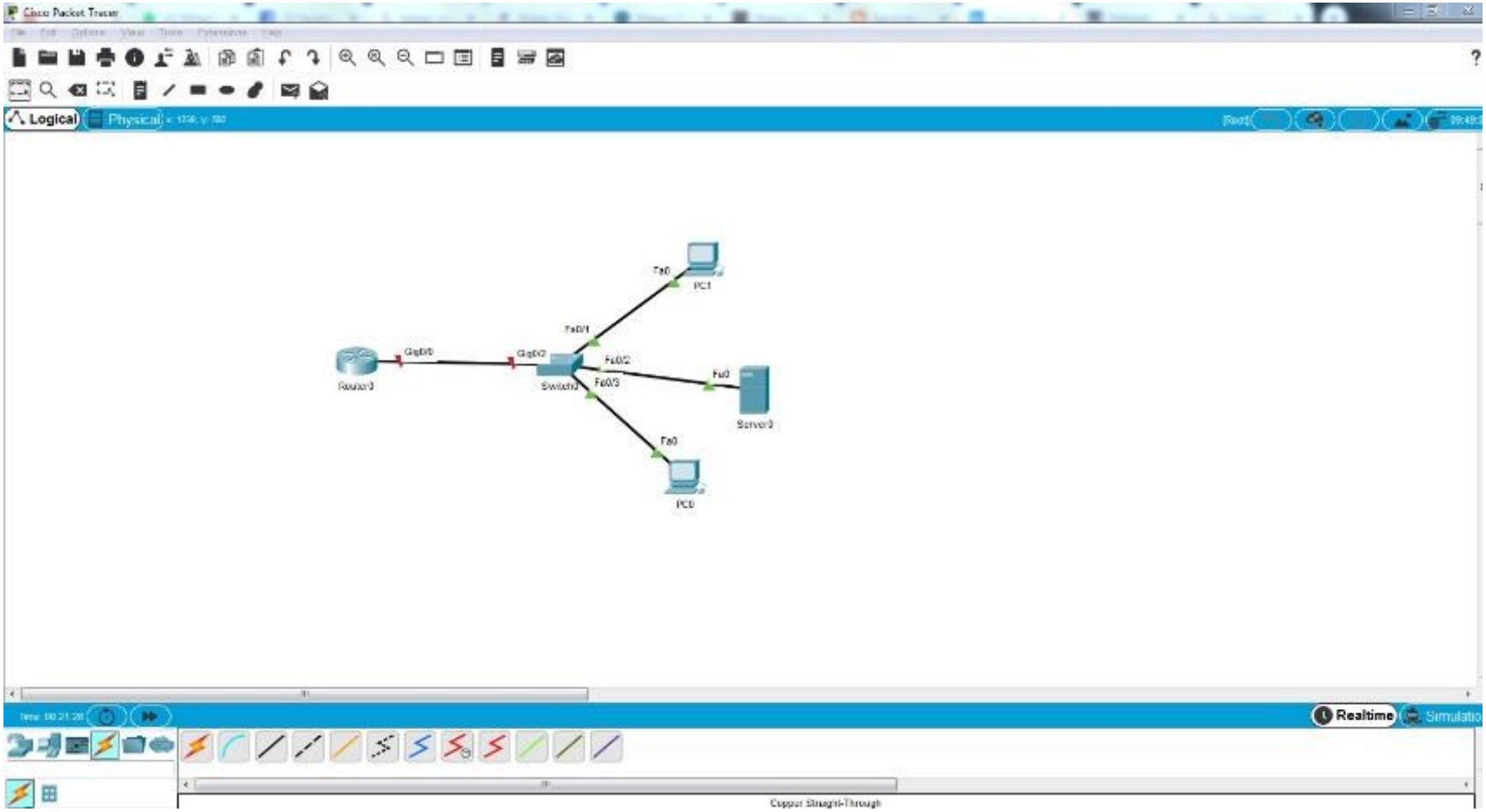
- Se matricular
  - Cursos > Packet Tracer > Ver Cursos > Getting Started with Cisco Packet Tracer
  - https://skillsforall.com/course/getting-started-cisco-packet-tracer
  - Start Today
  - Continue com NetAcad
  - Sign Up (Brazil, ano e mês de nascimento)
  - Continue
  - Aceitar e continuar
  - Browse Catalog
  - Getting Started With Cisco Packet Tracer
  - Get Started

Instalar o Packet Tracer

- Baixando
  - https://skillsforall.com/resources/lab-downloads
- Instale com a ferramenta
- Abra o programa
- Faça seu login do NetAcad

Tutorial Packet Tracer – WiFi!

- Acompanhe o tutorial!



ATIVIDADE

Atividade Avaliativa

- Grupos – 3 pontos na AV1
- Se inscreva no Cisco Network Academy
- Baixe o Cisco Packet Driver
- Escolha a casa de algum dos colegas que possui rede WiFi e modele essa rede no Packet Tracer
- Inicie um relatório, descrevendo a rede e as falhas, incluindo as possibilidades de ataques
- Configure a rede modelada para se tornar mais segura e detalhe no relatório.

ENCERRAMENTO

Resumo e Próximos Passos

- Funcionamento das redes WiFi
- Principais vulnerabilidades das redes WiFi
  - E os ataques associados
- Como proteger redes WiFi
- Tutorial Cisco Packet Tracer para WiFi
- **Pós Aula**: Aprenda Mais, Pós Aula e Desafio!
  - No padlet: https://padlet.com/djcaetano/segciber

- Detalhando algumas vulnerabilidades
  - Injeção, quebra de autenticação...

PERGUNTAS?