



# Zumbis, teias e negação de serviço

Uma introdução a DoS

# Alguns avisos

---



- Com grandes poderes vêm grandes responsabilidades

# Alguns avisos

---



- Com grandes poderes vêm grandes responsabilidades
- Tenha o conhecimento como objetivo

# Alguns avisos

---



- Com grandes poderes vêm grandes responsabilidades
- Tenha o conhecimento como objetivo
- Não faça merda

# Sobre o Ganesh

---



- Reversa
- Web
- Crypto
- REDES





Antes de começarmos...

# Martinez



- 1 parte Gin
- 2 partes Vermute seco
- Suco de cereja
- Rodela de limão



# Martinez



- ~~1 parte Gin~~
- 2 partes Gin
- 2 partes Vermute seco
- Suco de cereja
- Rodela de limão





# Martinez



- ~~1 parte Gin~~
- 2 partes Gin
- ~~2 partes Vermute seco~~
- 1 parte Vermute seco
- Suco de cereja
- Rodela de limão



# Martinez



- ~~1 parte Gin~~
- 2 partes Gin
- ~~2 partes Vermute seco~~
- 1 parte Vermute seco
- ~~Suco de cereja~~
- Rodela de limão



# Martinez



- ~~1 parte Gin~~
- 2 partes Gin
- ~~2 partes Vermute seco~~
- 1 parte Vermute seco
- ~~Suco de cereja~~
- ~~Rodela de limão~~



# Martinez



- ~~1 parte Gin~~
- 2 partes Gin
- ~~2 partes Vermute seco~~
- 1 parte Vermute seco
- ~~Suco de cereja~~
- ~~Rodela de limão~~
- Azeitona



# Martini!



- ~~1 parte Gin~~
- 2 partes Gin
- ~~2 partes Vermute seco~~
- 1 parte Vermute seco
- ~~Suco de cereja~~
- ~~Rodela de limão~~
- Azeitona





DoS == Denial of Service



# Historinhas sobre Dos

# Historinhas sobre DoS: 1



- Estônia, abril de 2007
- Governo quase 100% computadorizado
- Rússia vs Estônia?





# Historinhas sobre DoS: 2



- Github, 2015
- Projetos para burlar censura chinesa
- Baidu search engine



# Historinhas sobre DoS: 3 (última, prometo)



- Mirai botnet, 2016
- Dyn (provedor de DNS)
- Julian Assange?




# Historinhas sobre DoS: 3 (última, prometo)



- Mirai botnet, 2016
- Dyn (provedor de DNS)
- Julian Assange?

Internet of Things

”The S in **IoT** stands for Security”

A close-up photograph of a network switch or patch panel. Several white Ethernet cables are plugged into the top ports. The device is mounted on a metal rack. A semi-transparent dark grey rounded rectangle is overlaid on the center of the image, containing white text.

# Internet, Web, protocolos e outros conceitos

# Internet

# Web



# Internet

# Web



- Infraestrutura
- Rede
- 1969
- IP (Internet Protocol)



# Internet

- Infraestrutura
- Rede
- 1969
- IP (Internet Protocol)

# Web

- HTML
- Aplicação
- 1989
- HTTP/HTTPS (em geral)  
Protocol)

# Protocolos de comunicação

---





# Protocolos de comunicação



- Padrão de comunicação
  - Câmbio
  - Copiei
  - Câmbio, desligo



# Protocolos de comunicação

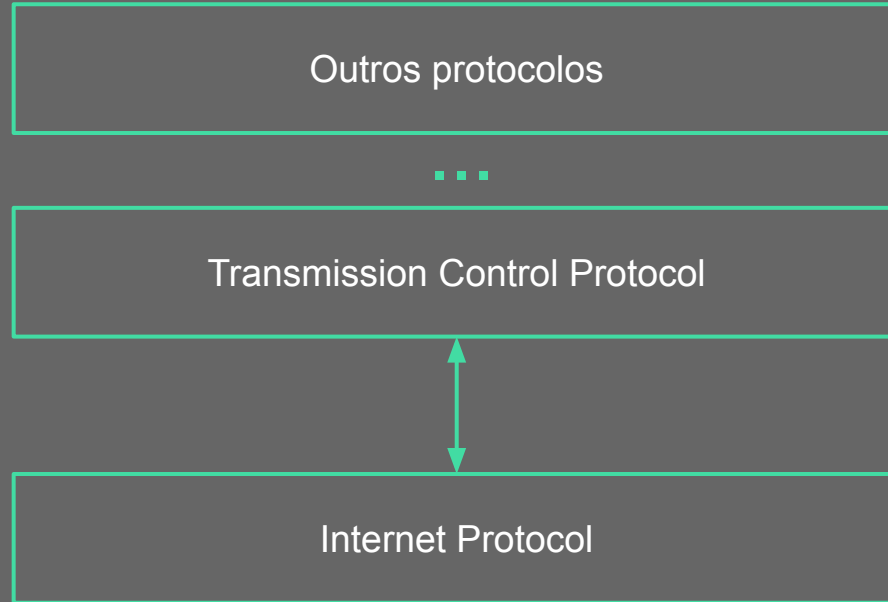


- Padrão de comunicação
  - Câmbio
  - Copiei
  - Câmbio, desligo
- Flexibilidade
  - Independe do hardware/software



# Protocol Stack (Pilha de protocolos)

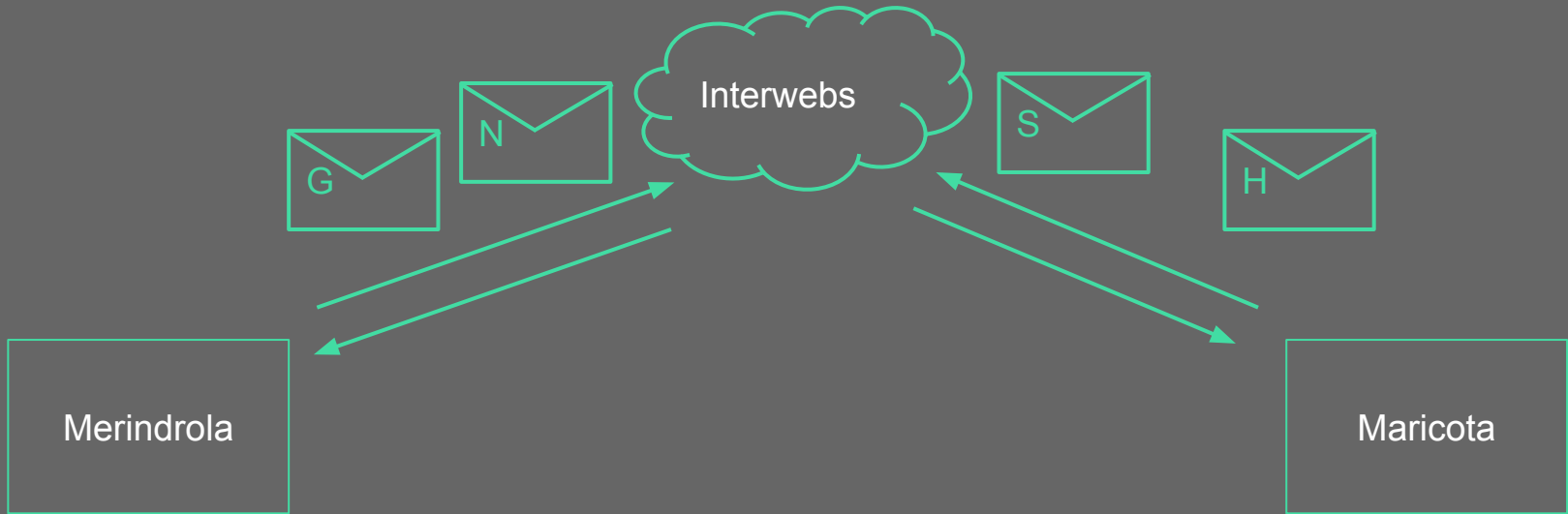
---





# IETF e RFCs

# Pacotes



# Arquitetura Cliente/Servidor

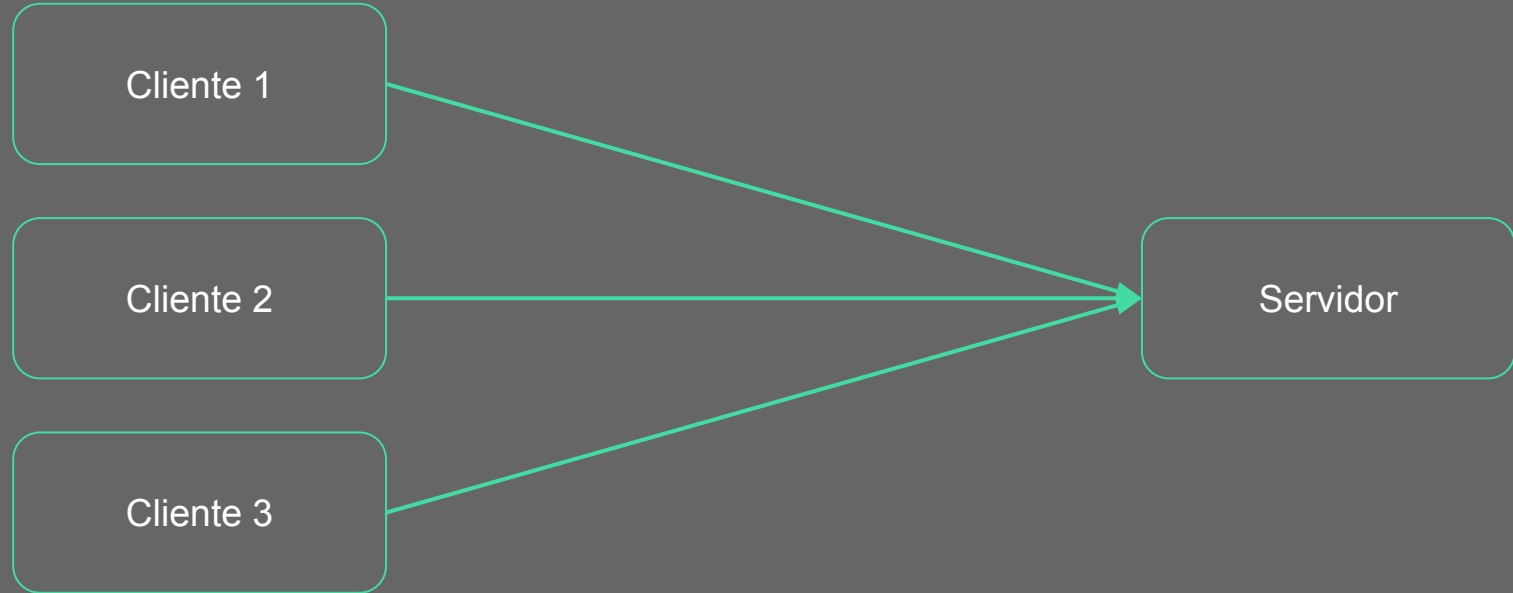
---



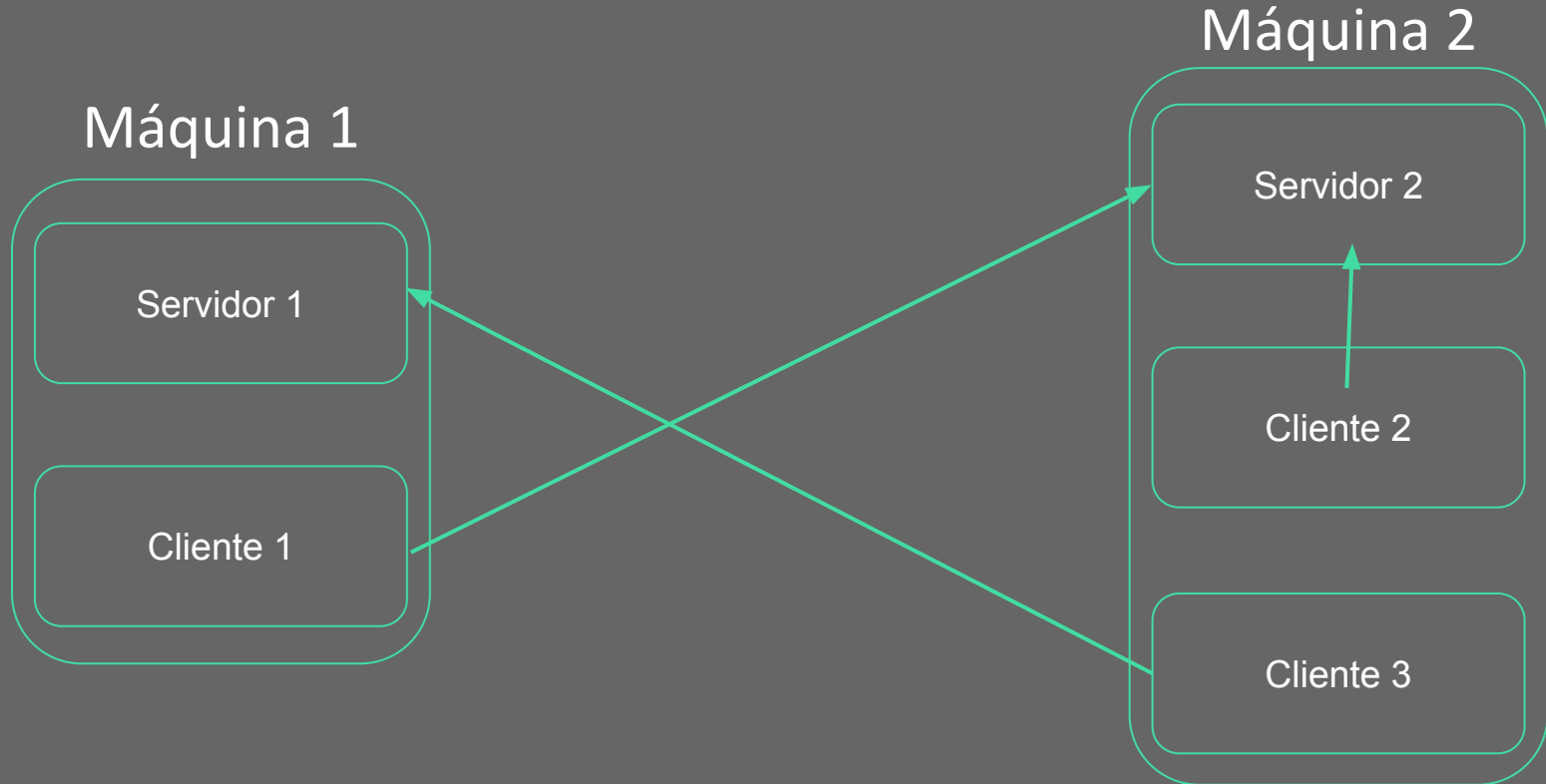
- **Cliente:** Máquina ou processo que utiliza ou demanda recursos ou serviços dos servidores
  - Browser
  - Cliente do LoL
- **Servidor:** Máquina ou processo que oferece algum tipo de serviço aos clientes
  - Servidor Web
  - Servidor DHCP
  - Servidor DNS

# Arquitetura Cliente/Servidor

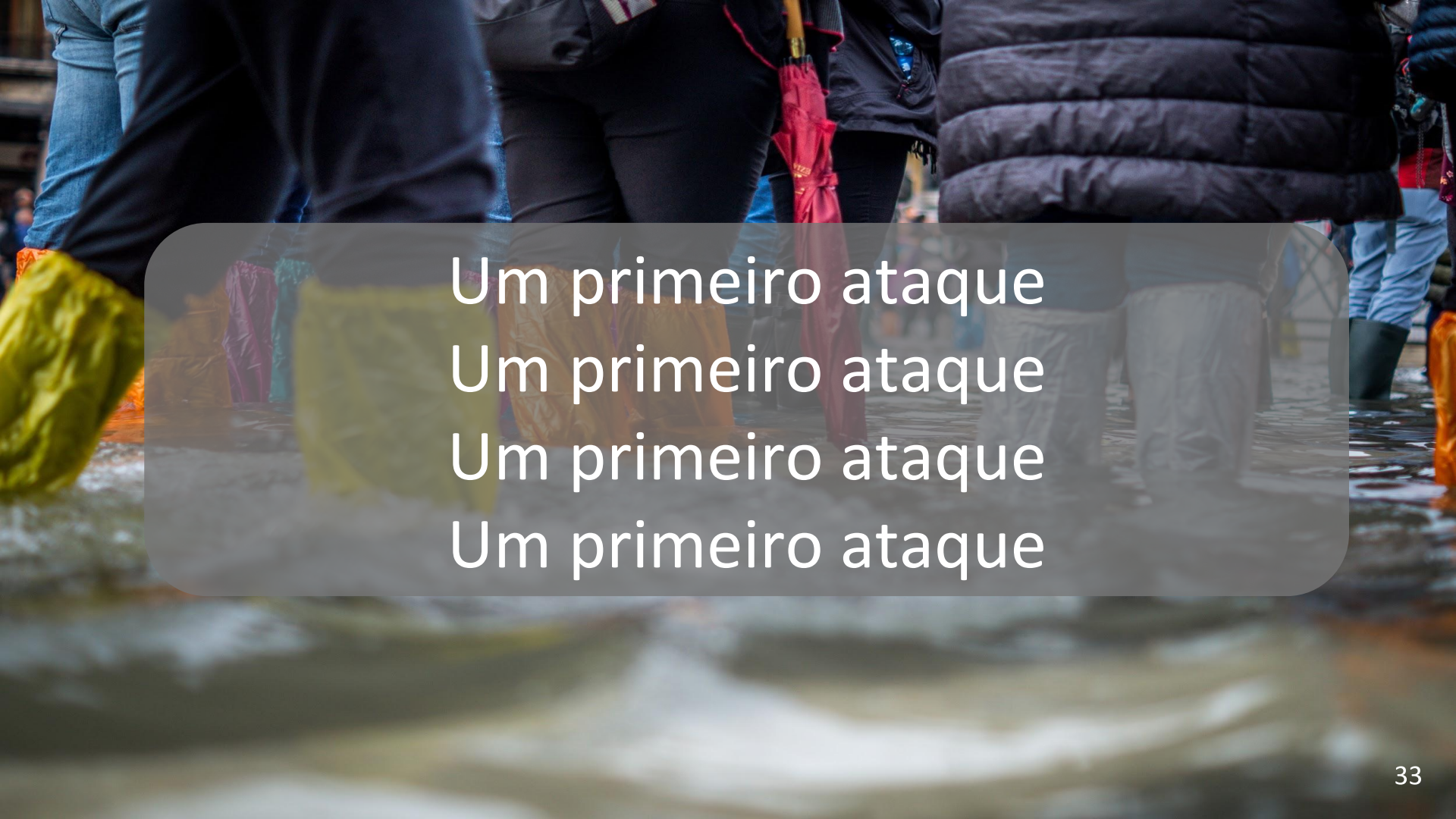
---



# Arquitetura Cliente/Servidor

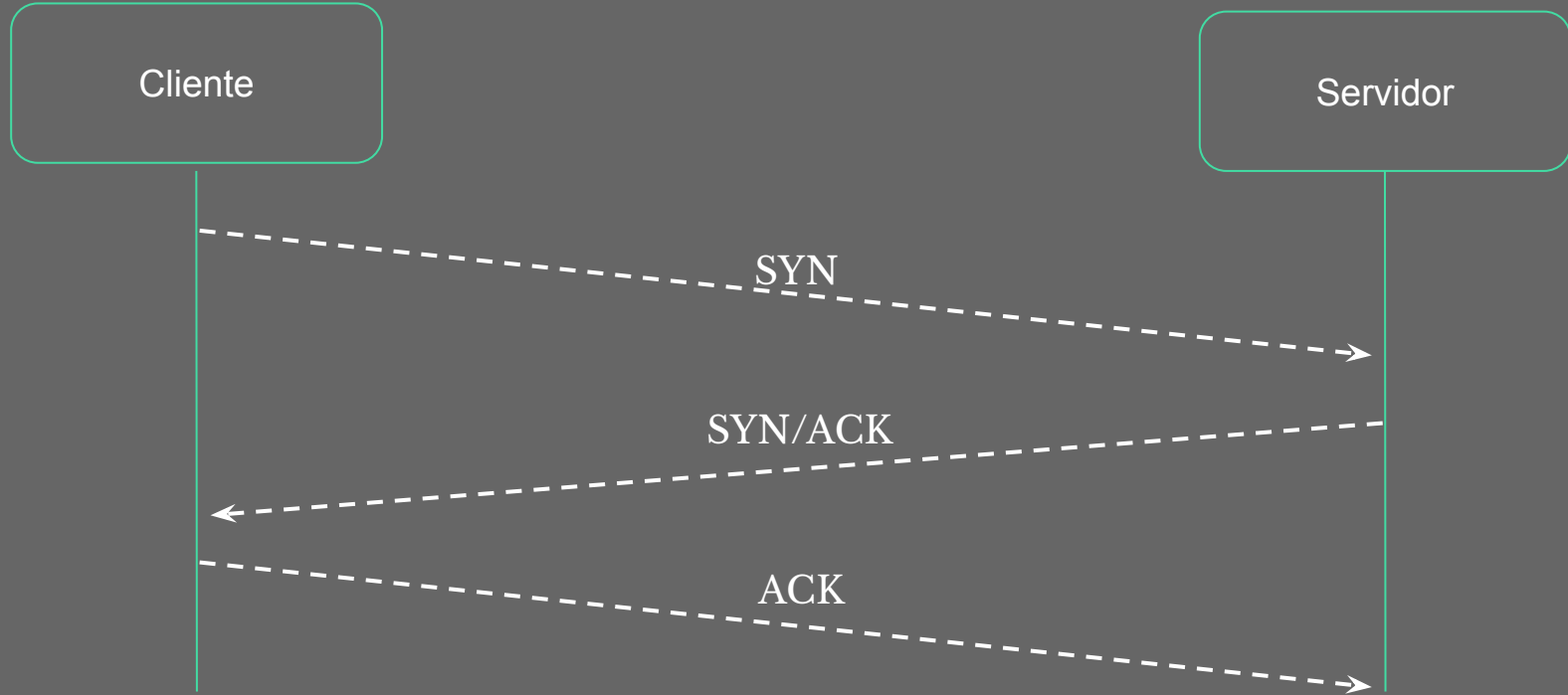




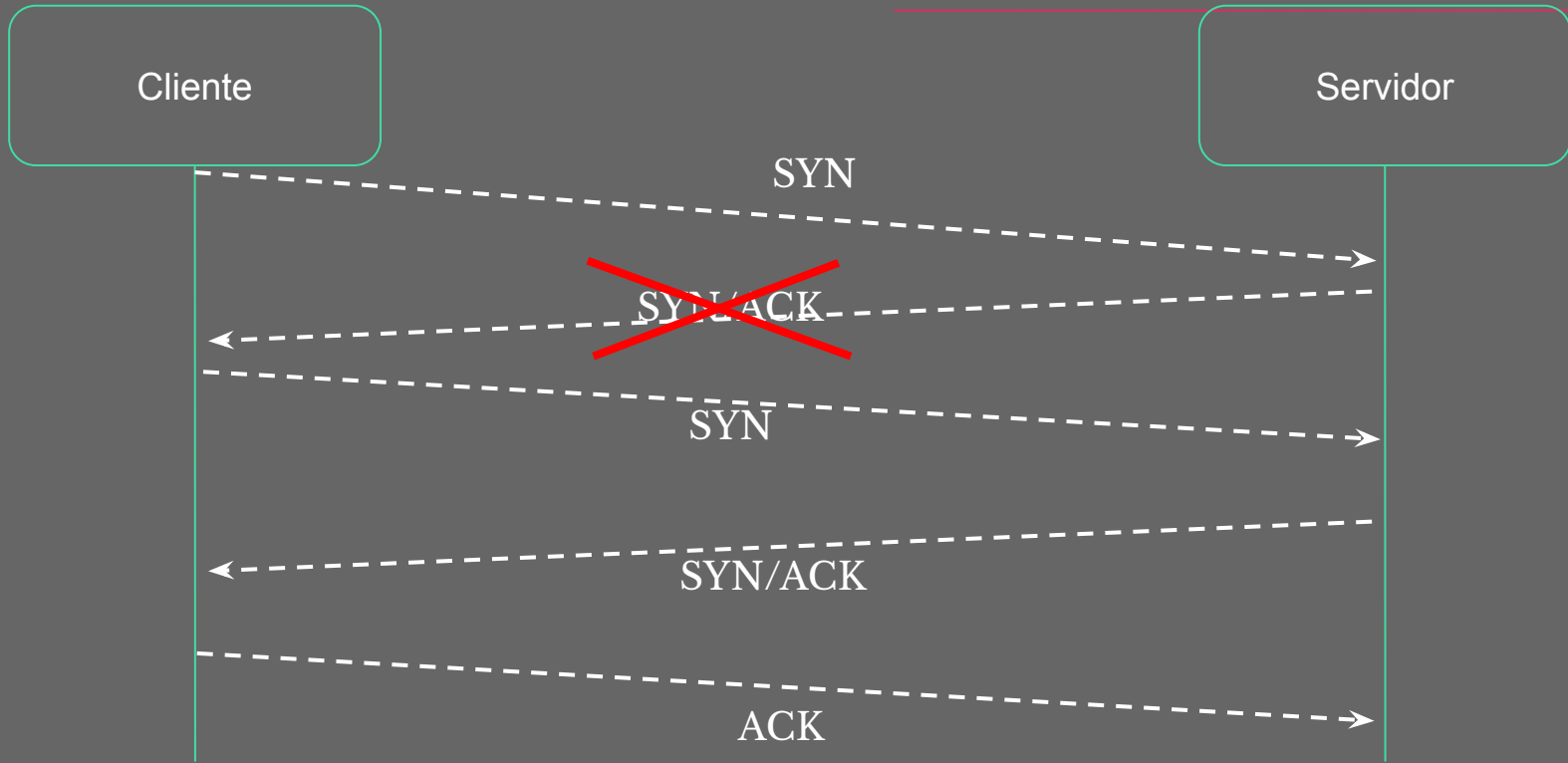
A group of people are wading through shallow, rippling water. They are wearing various types of waders and carrying gear. In the foreground, a person is wearing bright yellow waders. To their right, another person is wearing dark waders and carrying a red bag. Further back, a person is wearing a dark, quilted jacket and light-colored waders. The water is shallow and reflects the light, creating a shimmering effect. The background is slightly blurred, showing more people and what appears to be a wooden structure or fence.

Um primeiro ataque  
Um primeiro ataque  
Um primeiro ataque  
Um primeiro ataque

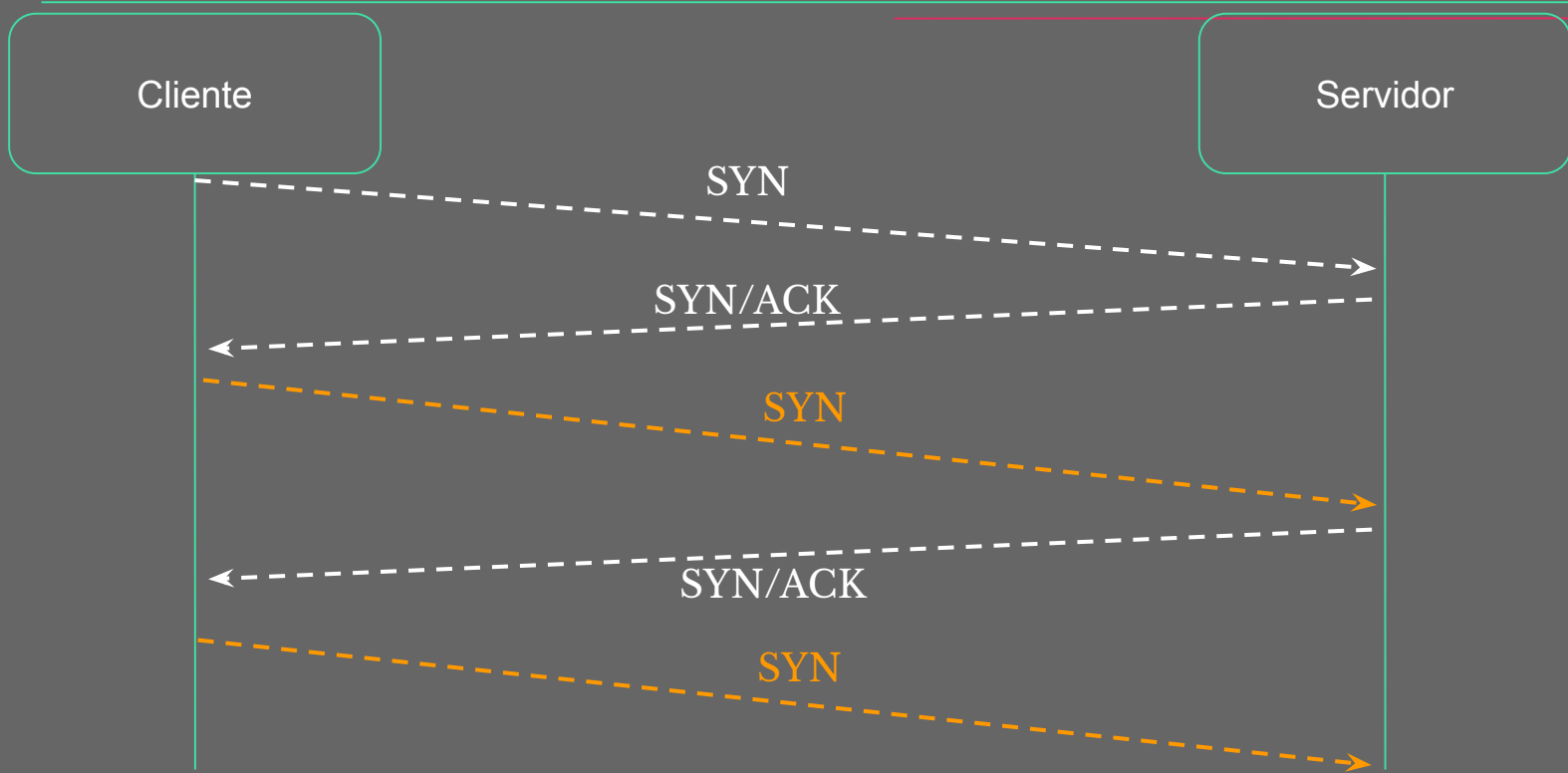
# Three-way handshake

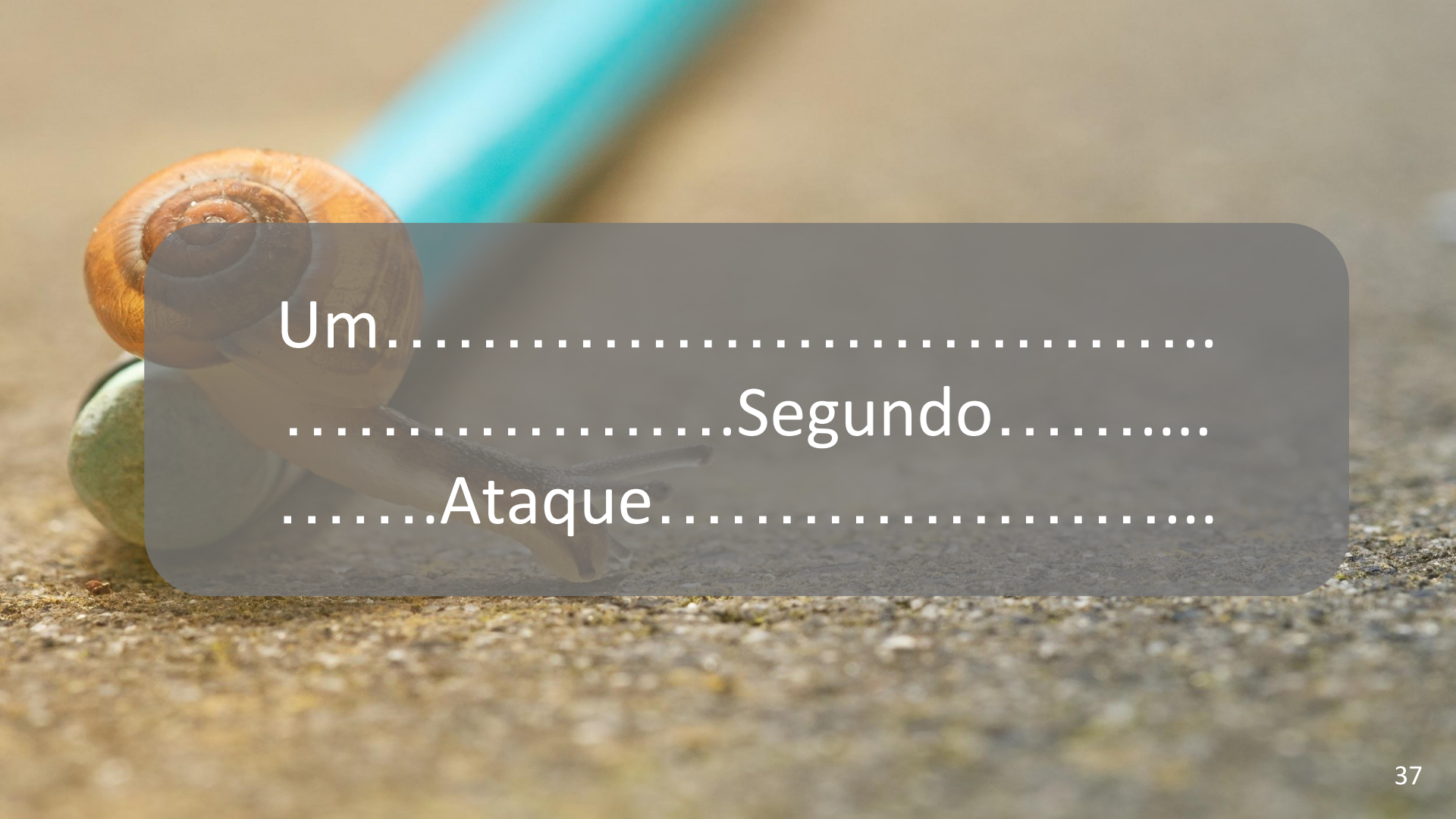


# Three-way handshake gone wrong



# SYN Flood

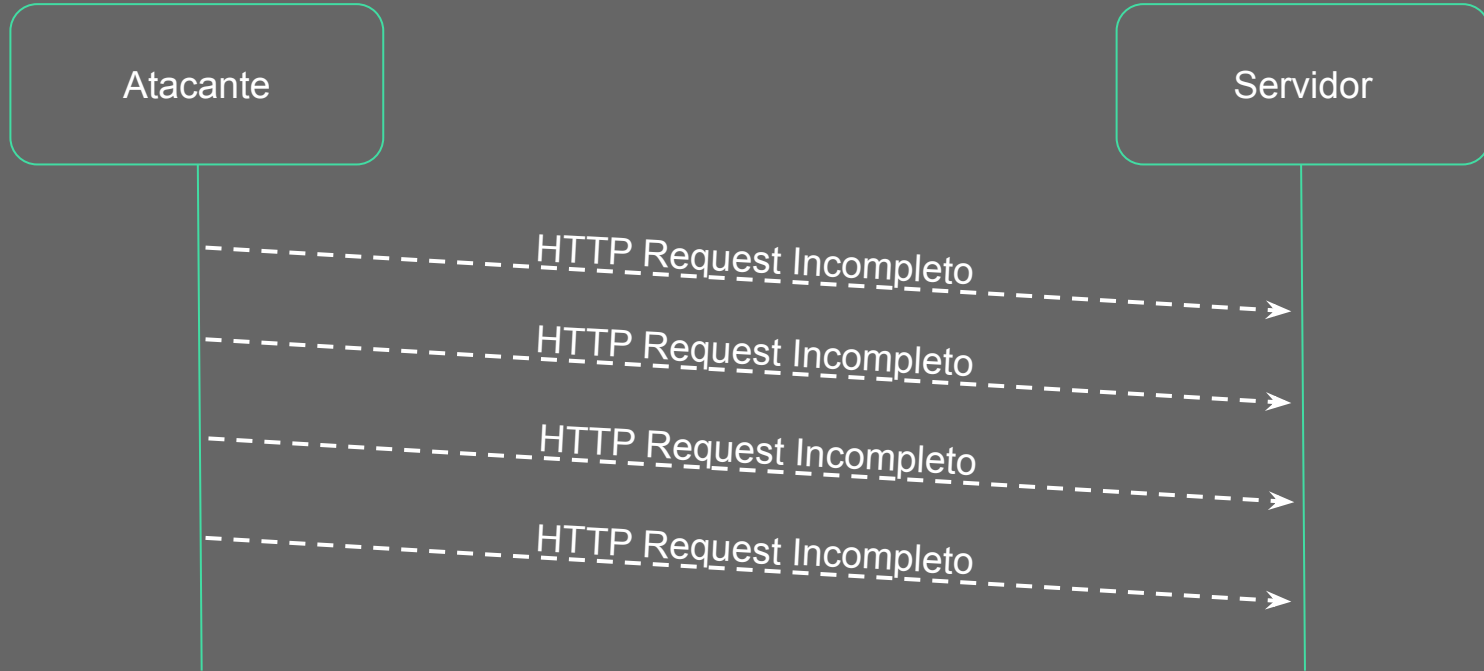




Um .....  
.....Segundo.....  
.....Ataque.....



# Slow Loris



A photograph of a lizard perched on top of a weathered wooden sign. The sign is painted blue and has the word "STOP" written in large, white, block letters. The sign is mounted on a wooden post. The background is a blurred natural setting with rocks and vegetation.

Antes do nosso próximo ataque



# DoS, ADoS, DDoS e Botnets

---



# DoS, ADoS, DDoS e Botnets

---



- DoS == Denial of Service (Negação de Serviço)

# DoS, ADoS, DDoS e Botnets

---



- DoS == Denial of Service (Negação de Serviço)
- **A**DoS == **Amplified** Denial of Service (Amplificado)

# DoS, ADoS, DDoS e Botnets

---



- DoS == Denial of Service (Negação de Serviço)
- **A**DoS == **Amplified** Denial of Service (Amplificado)
- **D**DoS == **Distributed** Denial of Service (Distribuído)

# DoS, ADoS, DDoS e Botnets

---



- DoS == Denial of Service (Negação de Serviço)
- **A**DoS == **Amplified** Denial of Service (Amplificado)
- **D**DoS == **Distributed** Denial of Service (Distribuído)
- Botnet == Rede de máquinas infectadas (bots)

# Ou seja...

---



# Ou seja...

---



- Nem todo DoS é um DDoS
  - Mas todo DDoS é um DoS

# Ou seja...

---



- Nem todo DoS é um DDoS
  - Mas todo DDoS é um DoS
- Nem todo DoS é um ADoS
  - Mas todo ADoS é um DoS



# Ou seja...

---



- Nem todo DoS é um DDoS
  - Mas todo DDoS é um DoS
- Nem todo DoS é um ADoS
  - Mas todo ADoS é um DoS
- Nem toda botnet faz DDoS

# Ou seja...

---



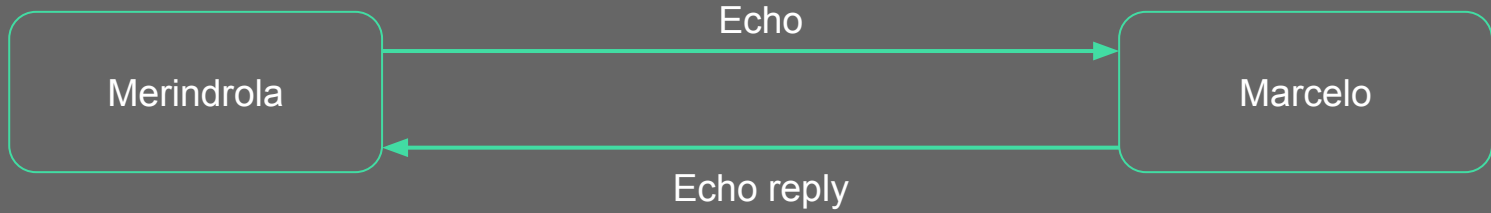
- Nem todo DoS é um DDoS
  - Mas todo DDoS é um DoS
- Nem todo DoS é um ADoS
  - Mas todo ADoS é um DoS
- Nem toda botnet faz DDoS
  - Mas dá pra fazer
- Nem todo DDoS é feito por uma botnet
  - Anonymous

A person is shown from the chest up, wearing a dark jacket with light-colored wavy patterns. They are holding a magnifying glass over their face, looking through the lens. They are also wearing bright blue sunglasses. The background is a blurred outdoor setting with trees and a building.

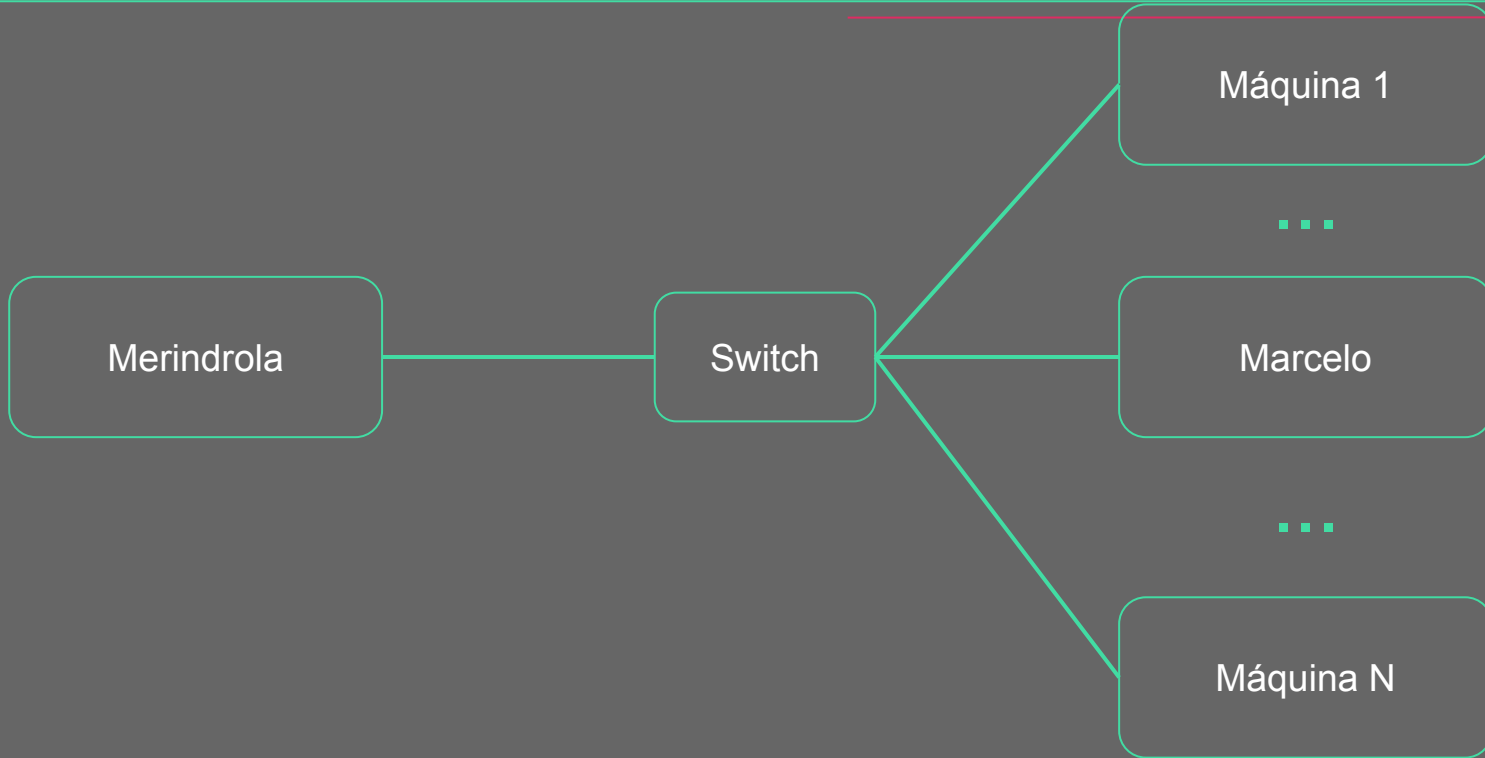
# o terceiro ataque

# ICMP Ping normal

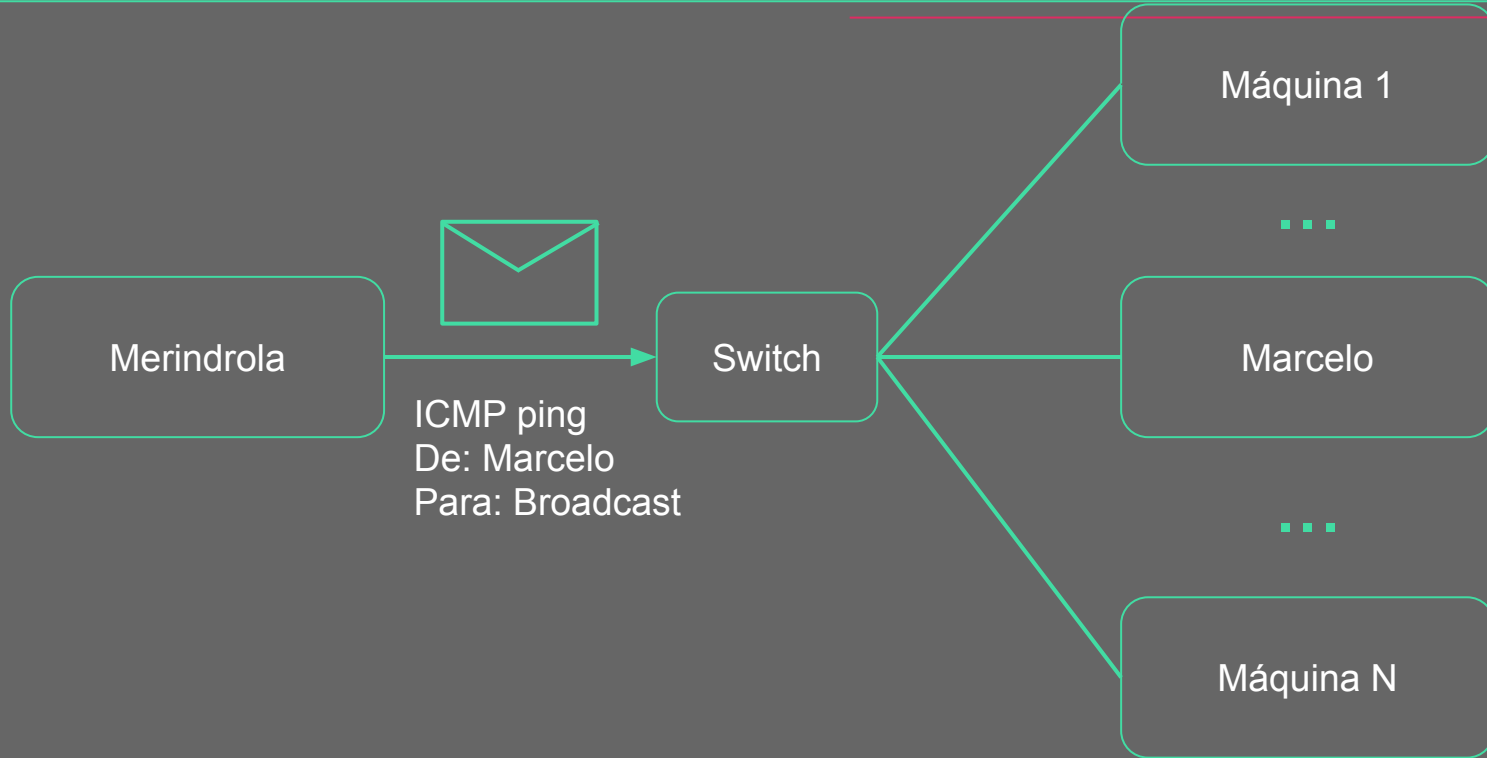
---



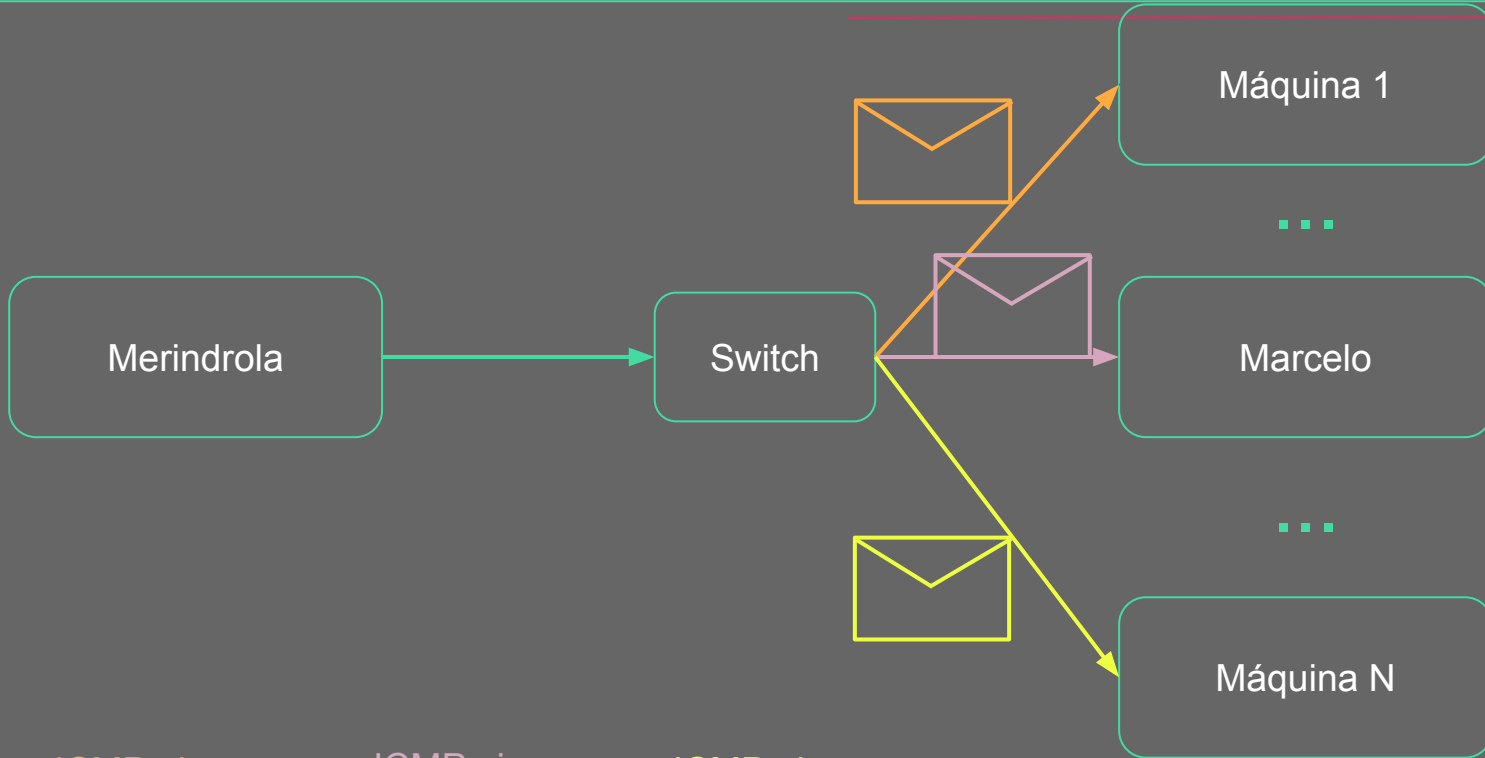
# ICMP Storm (Smurf Attack)



# ICMP Storm (Smurf Attack)



# ICMP Storm (Smurf Attack)

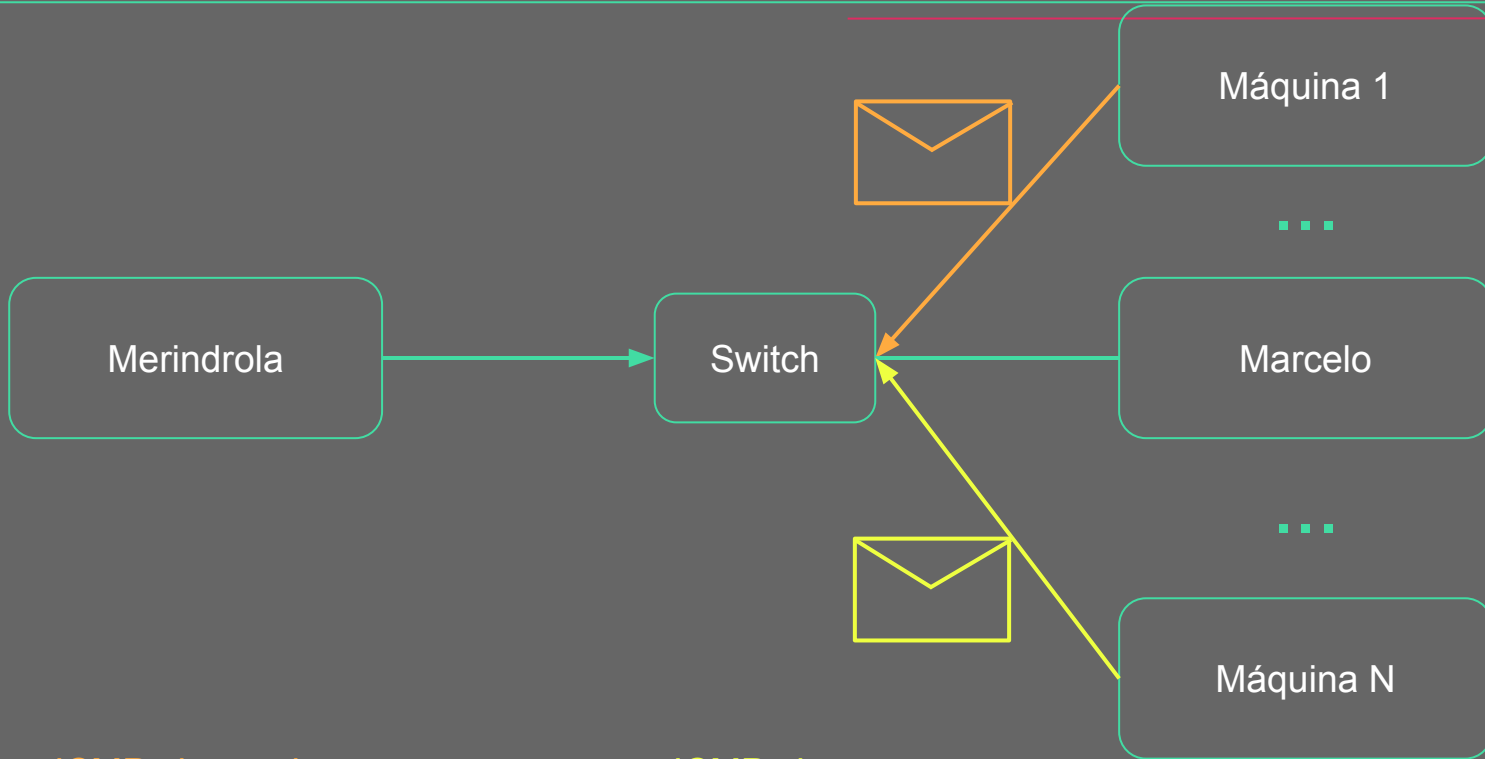


ICMP ping  
De: Marcelo  
Para: Máquina 1

ICMP ping  
De: Marcelo  
Para: Marcelo

ICMP ping  
De: Marcelo  
Para: Máquina N

# ICMP Storm (Smurf Attack)

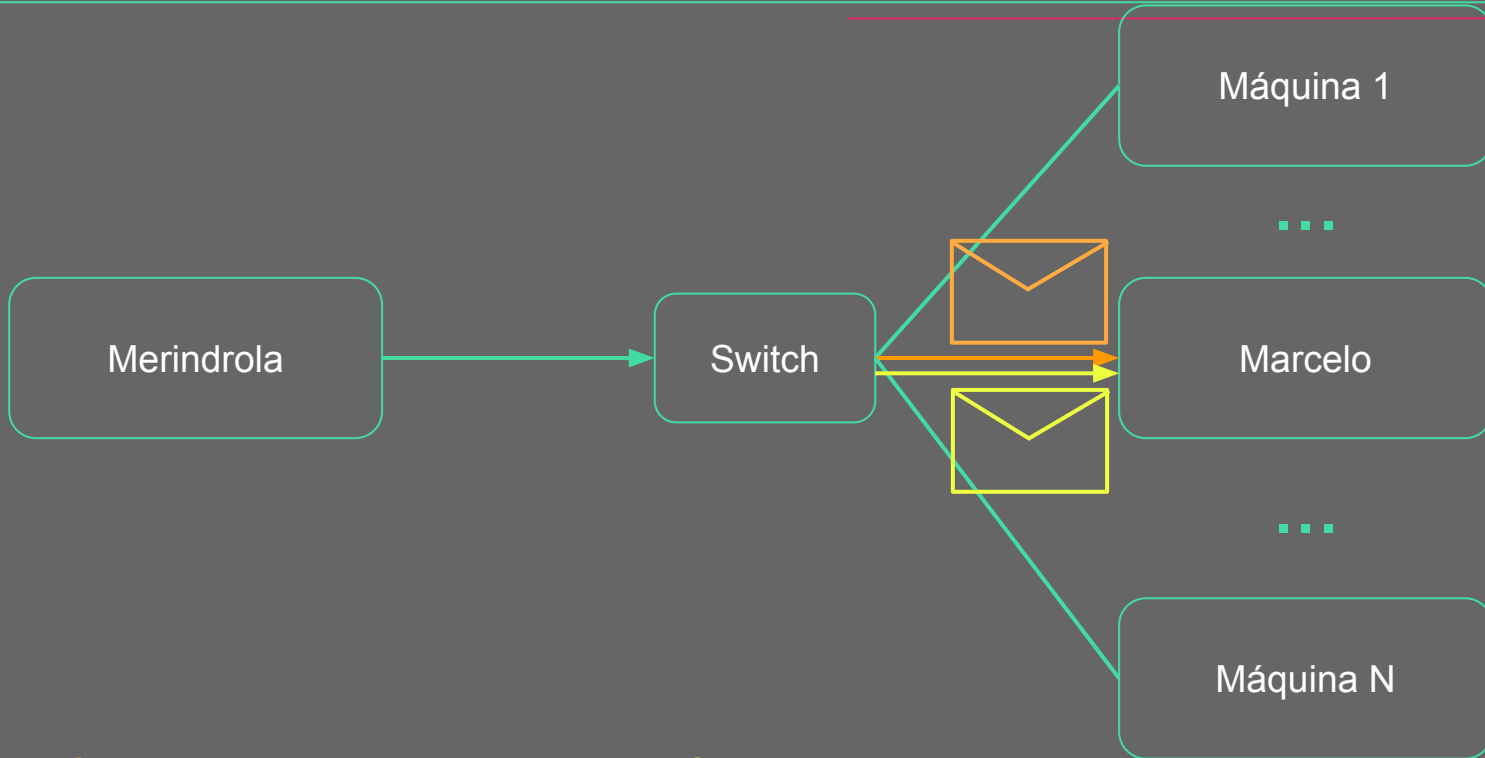


ICMP ping reply  
De: Máquina 1  
Para: Marcelo

ICMP ping  
De: Máquina N  
Para: Marcelo



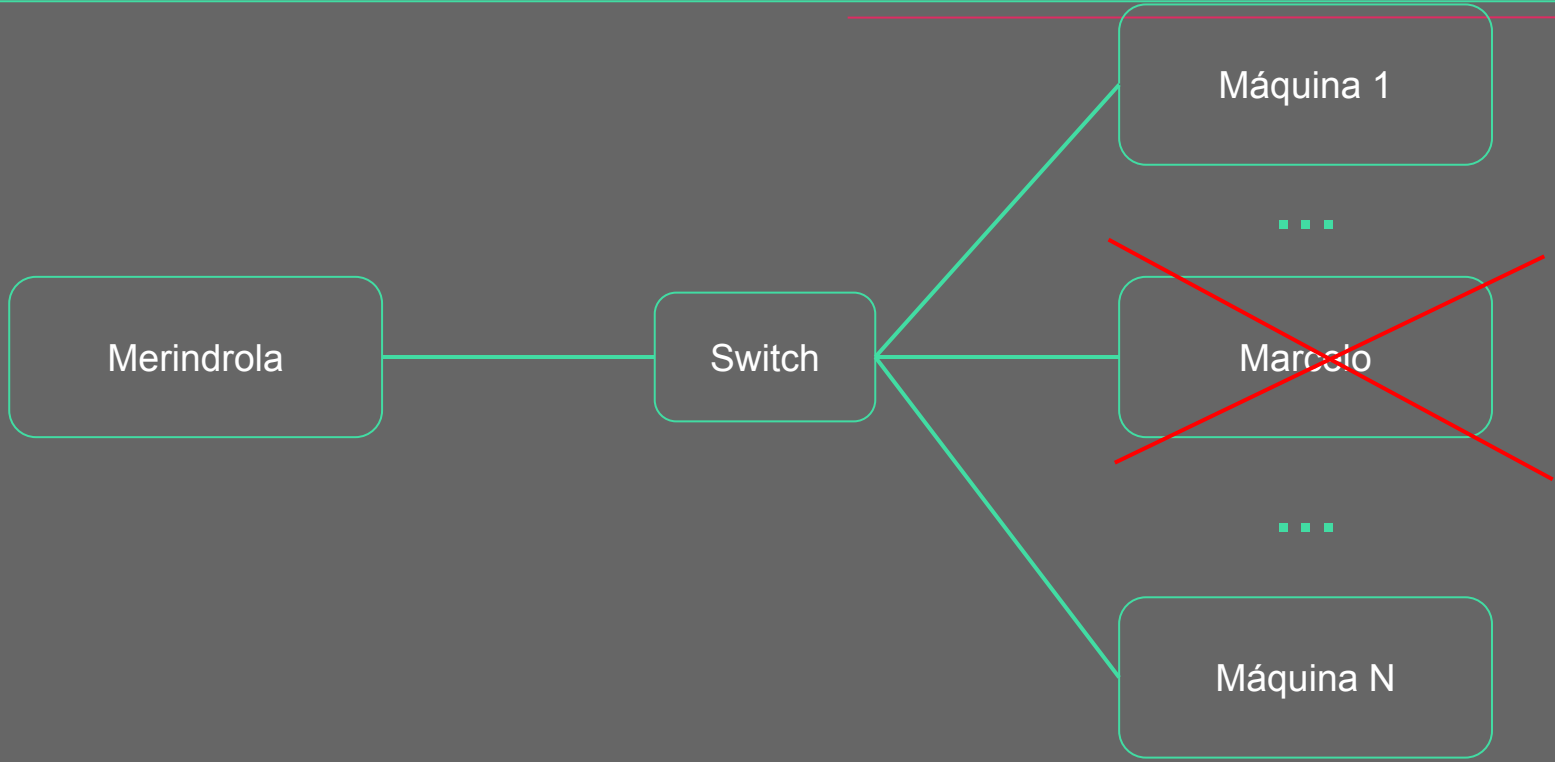
# ICMP Storm (Smurf Attack)



ICMP ping reply  
De: Máquina 1  
Para: Marcelo

ICMP ping  
De: Máquina N  
Para: Marcelo

# ICMP Storm (Smurf Attack)





# DDoS, Botnets e C&C

# Botnets

---



- Malware (Malicious Software)
  - Geralmente vírus
- Bots são as máquinas infectadas
- Botnets podem ser voluntárias (Anonymous)
  - Low Orbit Ion Cannon (LOIC)
- Botmaster controla os bots

# Botnets

---



- Malware (Malicious Software)
  - Geralmente vírus
- Bots são as máquinas infectadas
- Botnets podem ser voluntárias (Anonymous)
  - Low Orbit Ion Cannon (LOIC)
- Botmaster controla os bots (Como???)

# Command and Control (C&C)

---



- Centralizado
  - Canal IRC
  - Website
  
- Descentralizado
  - Redes peer-to-peer (P2P)
  - Distributed Hash Tables (DHT)

# Obrigado!

---



- Material adicional
  - Slides do minicurso: [tiny.cc/ganeshdosslides](https://tiny.cc/ganeshdosslides)
  - Material escrito: [tiny.cc/ganeshdoshackmd](https://tiny.cc/ganeshdoshackmd)
  
- Gabriel Cruz (Eu!)
  - LinkedIn: [linkedin.com/in/gabriel-de-melo-cruz/](https://linkedin.com/in/gabriel-de-melo-cruz/)
  - Github: [github.com/gmelodie](https://github.com/gmelodie)

# GANESH

Grupo de Segurança da Informação  
ICMC / USP - São Carlos, SP  
<http://ganesh.icmc.usp.br/>  
[ganesh@icmc.usp.br](mailto:ganesh@icmc.usp.br)

