



# Protocolo 802.1AE (MACSec): Segurança do Fluxo de Dados sem Perda de Performance

*Quinta às Quinze 21/03/2024*

Elvio de Sousa



Engineer @ Cisco | Msc | ITQ | 5x CCNP

Gabriel Almeida



Engineer @ Cisco | CCNA

# Laboratório de Transferência Tecnológica (LTT)

## Visão de sua arquitetura



SD-Access  
Cisco DNA Center



SD-WAN  
Cisco vManage



ACI  
Cisco APIC

LAN /  
ROBO



Usuários & Dispositivos

- Acesso Seguro
- Automação da Rede
- Facilidade na operação
- Informações de telemetria

WAN



Transporte de Dados

- Comportamento adaptativo
- Melhor experiência das aplicações
- Segurança no acesso à Internet

Data  
Center



Dados & Aplicações

- Automação e integração de recursos
- Prevenção de violações de segurança
  - DevOps

Outras soluções: MERAKI, Segurança, AppDynamics, ThousandEyes, etc.

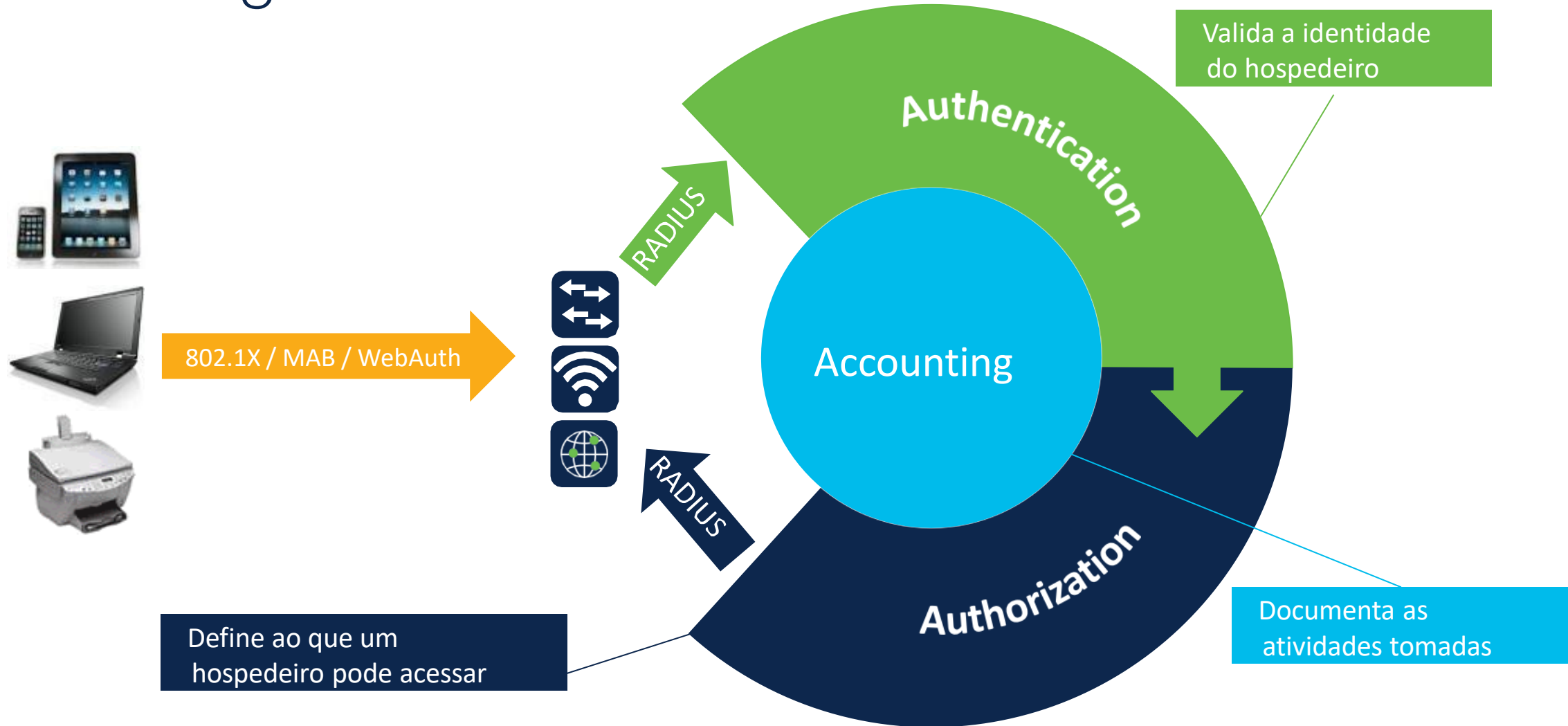
- Introdução ao Protocolo 802.1x
- Características 802.1AE e suas Vantagens
- MACSec vs IPSec
- 802.1x Session Hijacking e MACSec

# AGENDA

# Fundamentos de AAA



# Authentication, Authorization and Accounting

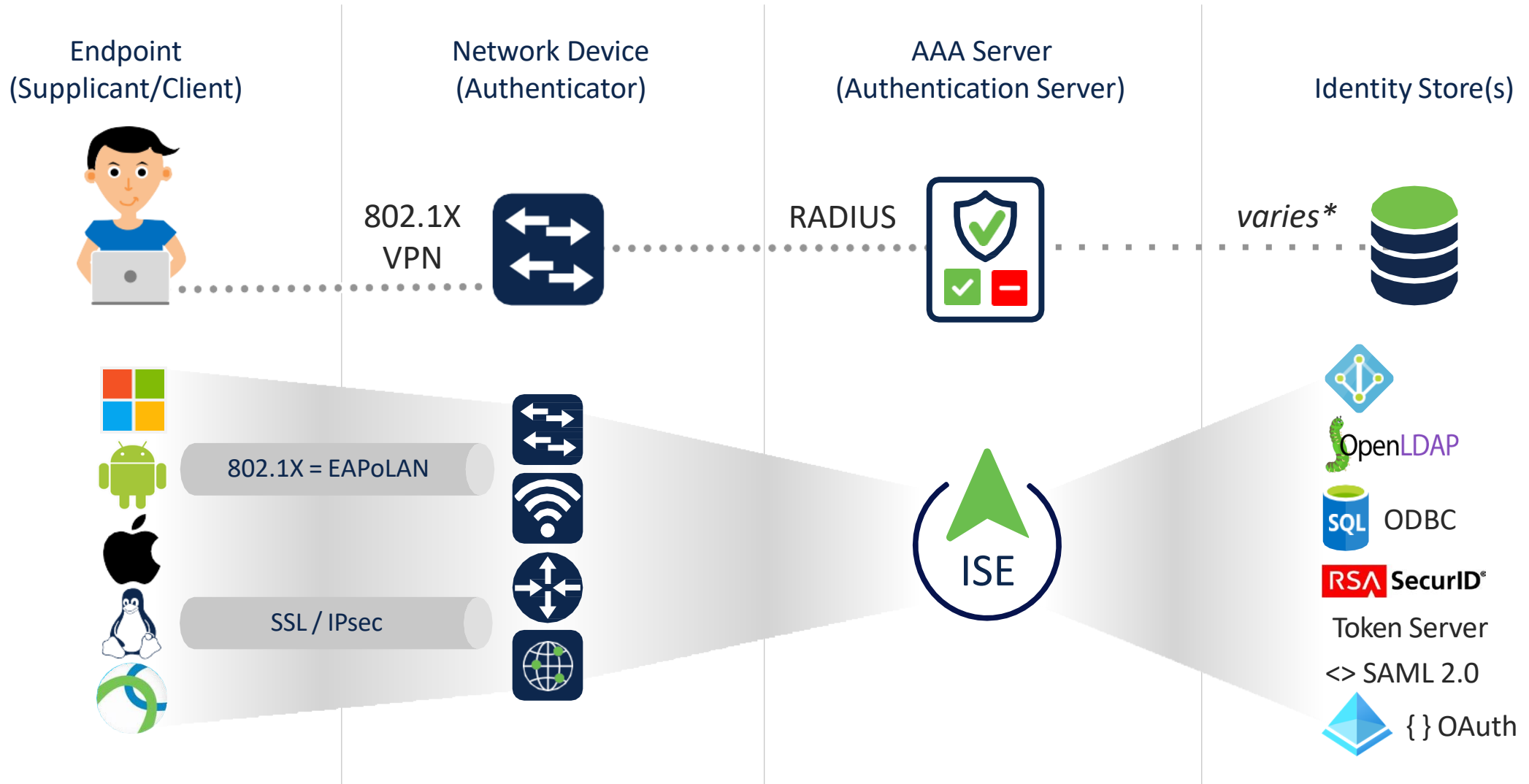


# Operação de um Servidor RADIUS

RADIUS = Remote Authentication Dial-In User Service



RFC2865 : RADIUS  
RFC2866 : Accounting  
RFC3579 : EAP Support  
RFC5176 : CoA Support





# O que é 802.1AE?

- **Media Access Control (MAC) Security**
  - Padrão IEEE 802.1AE - **2006** para proteção criptográfica forte da Camada 2
  - Mitiga ataques de snooping e spoofing
  - Protege a confidencialidade e a integridade dos dados em trânsito
    - Incluindo STP, CDP, OSPF, etc.
    - Criptografa o tráfego e permite a inspeção por dispositivos confiáveis
- **Protege a comunicação de componentes confiáveis na LAN**
  - Depende de 802.1X para gerenciamento de chaves, autenticação e controle de acesso
- **Projetado para implantação incremental**
  - Proteja primeiro os dispositivos mais vulneráveis
  - Minimiza o impacto na rede



No.	Time	Source	Destination	Protocol	Length	Info
271	132.452784	Dell_94:b6:00	IPv4mcast_16	MACSEC	86	MACsec frame
272	132.454014	Dell_94:b6:00	IPv4mcast_fc	MACSEC	100	MACsec frame
273	132.454024	Dell_94:b6:00	Broadcast	MACSEC	74	MACsec frame
274	132.456720	Dell_94:b6:00	Cisco_9f:f7:73	MACSEC	110	MACsec frame
275	132.495125	Dell_94:b6:00	Cisco_9f:f7:73	MACSEC	153	MACsec frame
276	132.517129	Dell_94:b6:00	Cisco_9f:f7:73	MACSEC	122	MACsec frame
277	132.541629	Dell_94:b6:00	Cisco_9f:f7:73	MACSEC	164	MACsec frame
278	132.743780	Dell_94:b6:00	IPv4mcast_16	MACSEC	86	MACsec frame
279	132.870407	Dell_94:b6:00	IPv4mcast_fc	MACSEC	100	MACsec frame
280	132.893203	Dell_94:b6:00	Cisco_9f:f7:73	MACSEC	108	MACsec frame
281	133.192649	Dell_94:b6:00	Cisco_9f:f7:73	MACSEC	106	MACsec frame
282	133.204133	Dell_94:b6:00	LLDP_Multicast	MACSEC	90	MACsec frame
284	133.234253	Dell_94:b6:00	Broadcast	MACSEC	74	MACsec frame
285	133.234611	Dell_94:b6:00	Cisco_9f:f7:73	MACSEC	106	MACsec frame
292	134.206220	Dell_94:b6:00	LLDP_Multicast	MACSEC	90	MACsec frame
293	134.238200	Dell_94:b6:00	Broadcast	MACSEC	74	MACsec frame
294	134.238558	Dell_94:b6:00	Cisco_9f:f7:73	MACSEC	106	MACsec frame
295	134.257169	Dell_94:b6:00	IPv4mcast_16	MACSEC	86	MACsec frame
296	134.263163	Dell_94:b6:00	IPv4mcast_16	MACSEC	86	MACsec frame
297	134.276819	Dell_94:b6:00	IPv4mcast_fb	MACSEC	106	MACsec frame
298	134.277408	Dell_94:b6:00	IPv4mcast_fc	MACSEC	100	MACsec frame

```

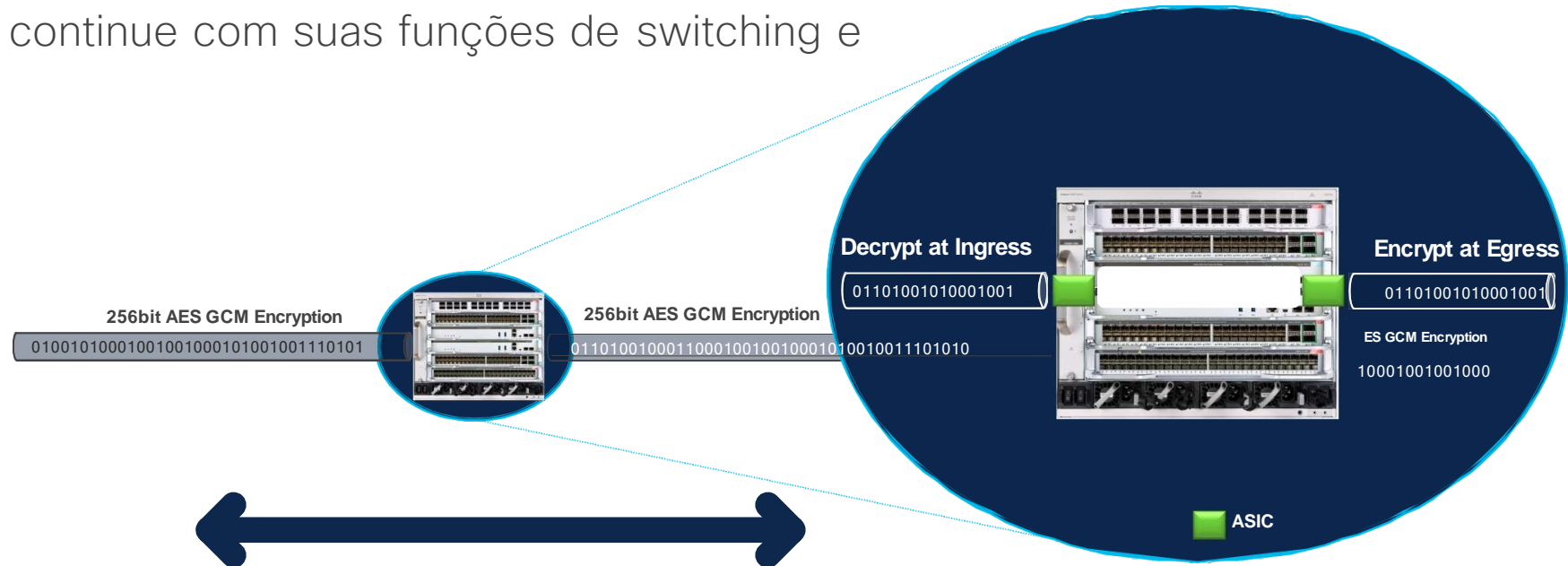
Frame 274: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface en6, id 0
  Section number: 1
  Interface id: 0 (en6)
    Interface name: en6
    Interface description: USB 10/100/1000 LAN
    Encapsulation type: Ethernet (1)
    Arrival Time: May 24, 2023 11:27:22.824615000 -03
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1684938442.824615000 seconds
    [Time delta from previous captured frame: 0.002696000 seconds]
    [Time delta from previous displayed frame: 0.002696000 seconds]
    [Time since reference or first frame: 132.456720000 seconds]
    Frame Number: 274
    Frame Length: 110 bytes (880 bits)
    Capture Length: 110 bytes (880 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:macsec:data]
  Ethernet II, Src: Dell_94:b6:00 (f0:4d:a2:94:b6:00), Dst: Cisco_9f:f7:73 (00:00:0c:9f:f7:73)
    Destination: Cisco_9f:f7:73 (00:00:0c:9f:f7:73)
      Address: Cisco_9f:f7:73 (00:00:0c:9f:f7:73)
        .... ..0. .... = LG bit: Globally unique address (factory default)
        .... ...0 .... = IG bit: Individual address (unicast)
    Source: Dell_94:b6:00 (f0:4d:a2:94:b6:00)
      Address: Dell_94:b6:00 (f0:4d:a2:94:b6:00)
        .... ..0. .... = LG bit: Globally unique address (factory default)
        .... ...0 .... = IG bit: Individual address (unicast)
    Type: 802.1AE (MACsec) (0x88e5)
  802.1AE Security tag
    0010 11.. = TCI: 0x0b, VER: 0x0, SC, E, C
      0... .... = VER: 0x0
      .0.. .... = ES: Not set
      ..1. .... = SC: Set
      ...0 .... = SCB: Not set
      .... 1... = E: Set
      .... .1.. = C: Set
      .... ..00 = AN: 0x0
    Short length: 0
    Packet number: 18
    System Identifier: Dell_94:b6:00 (f0:4d:a2:94:b6:00)
    Port Identifier: 0
    ICV: 09d985bf27af4b82bc4098817de394ba
  Data (66 bytes)
    Data: 59bf7c15b777262300c6c4fc5bfa4d94af15f6b85805fed9122631223c0c0569ff7324d6...
    [Length: 66]
  
```

- Captura pacotes 802.1AE

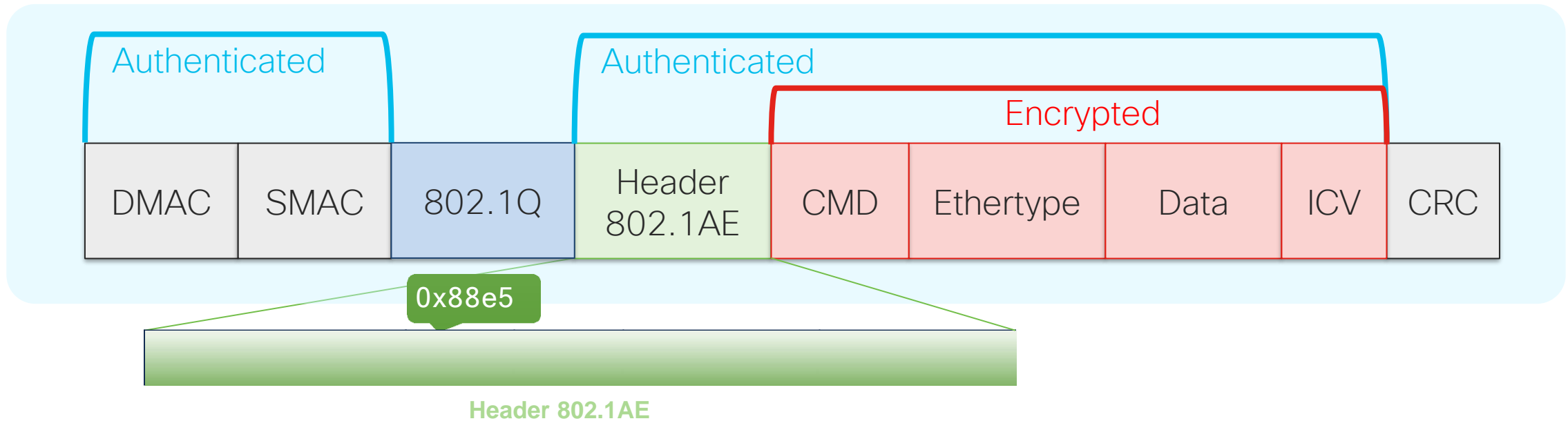
# Resumidamente,

802.1AE é sobre proteção salto a salto

- Modelo salto-à-salto vs ponta-à-ponta
  - Pacotes são decriptados na interface de entrada
  - Pacotes são encriptados na interface de saída
- Permite que a rede continue com suas funções de switching e roteamento

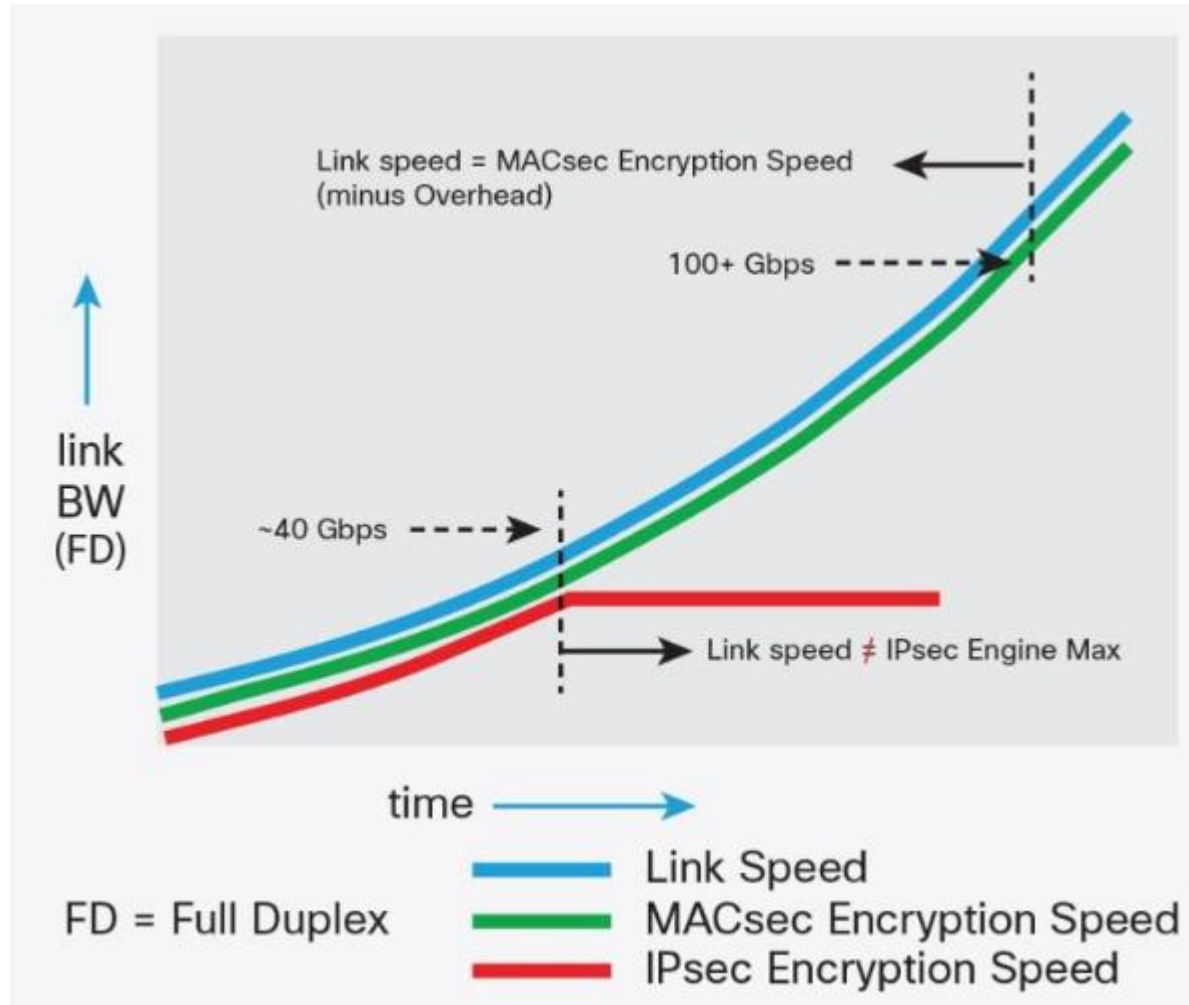


# Estrutura de um Frame 802.1AE para LAN



- Os quadros são criptografados e protegidos com um valor de verificação de integridade (ICV)
- O MACsec Ethertype é 0x88e5 (definido pelo IEEE 802.1AE)
- O MTU de IP é ajustado automaticamente para acomodar a tag MACsec de 32 B

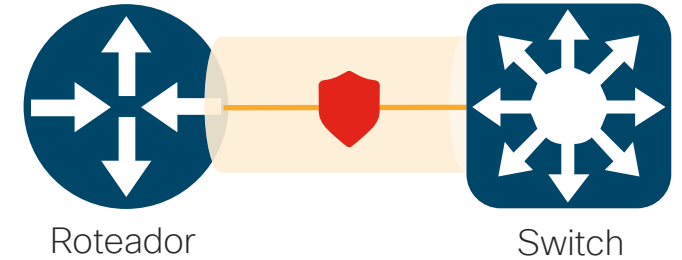
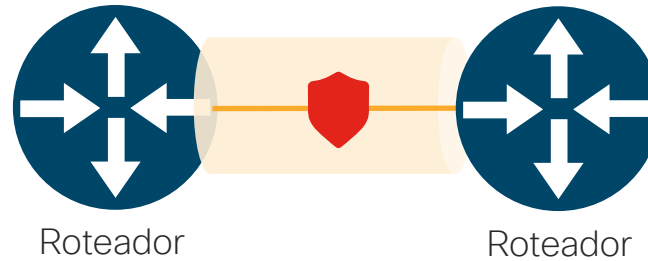
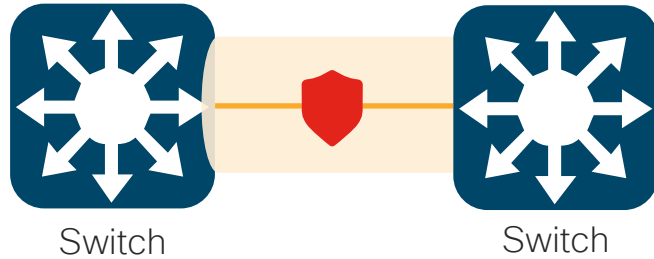
# Taxa de Transferência MACSec e IPsec



- Se uma implementação exigir que todo o tráfego que sai/passa pelo roteador precisa ser criptografado, a taxa de transferência do roteador agora será restrita ao desempenho do mecanismo IPsec.
- MACsec, como o nome indica, é a criptografia da camada MAC e oferece criptografia igual à das taxas de porta Ethernet (1/10/40) bidirecionalmente, independentemente do tamanho do pacote tamanho do pacote, executando a função de criptografia na camada física (PHY) da porta Ethernet.

# LAN MACsec

Encripta todo o trafego após o header 802.1Q



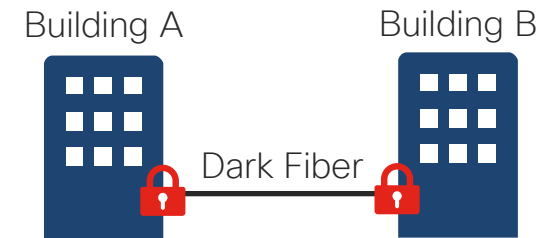
Onde podemos usar o LAN MACsec?



Instituições Financeiras

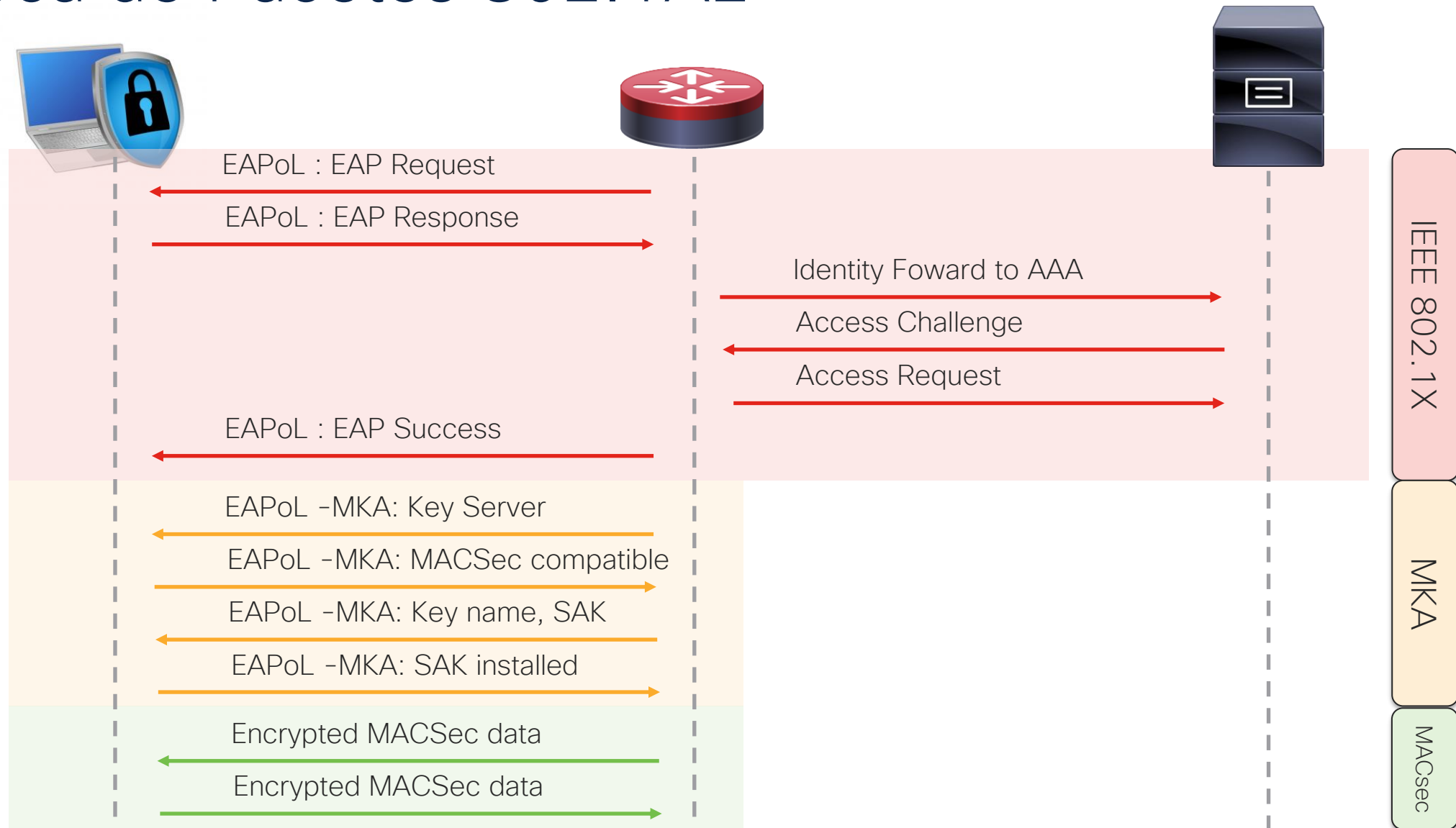


Sede Campus



Entre Sedes

# Troca de Pacotes 802.1AE



# Comaração MACSec com IPSec

	WAN MACsec	IPsec
Requisitos do link	Requer circuitos MetroE EVC dedicados para conexão L2 entre locais	Facilmente comutado entre tipos de link
Desempenho da criptografia	Linear (1 Gb/s, 10 Gb/seg, 40 Gb/seg, 100 Gb/seg)	Limitado pelo mecanismo de criptografia.
Impacto na ativação	Sem impacto na velocidade de criptografia	Menor taxa de transferência e criptografia
Por dimensionamento	Limitado por recursos de hardware	Altamente escalável
Taxa de transferência	Linear (1 Gb/s, 10 Gb/seg, 40 Gb/seg, 100 Gb/seg)	Taxa de transferência agregada (taxa de transferência + taxa de criptografia)
Facilidade de Uso	Configuração simples	Opções complexas disponíveis, mas configuração complexa.
Monitoramento de camada 3	Não visível para monitoramento de camada 3, com exceção de cabeçalhos de camada 2 e tags VLAN/MPLS.	Monitoramento de camada 3 e altamente visível disponível
Compatibilidade NAT/PAT	Cabeçalho de camada 3 inacessível, portanto, incompatível com NAT no link.	Funciona com soluções NAT

# 802.1x

## Session Hijacking Lab







Ajudando as empresas na proteção contra ataques...

Reposted from Fernando Z. • 1mo • 🌐

Exemplo do  
Ataque

# Invasão de Redes

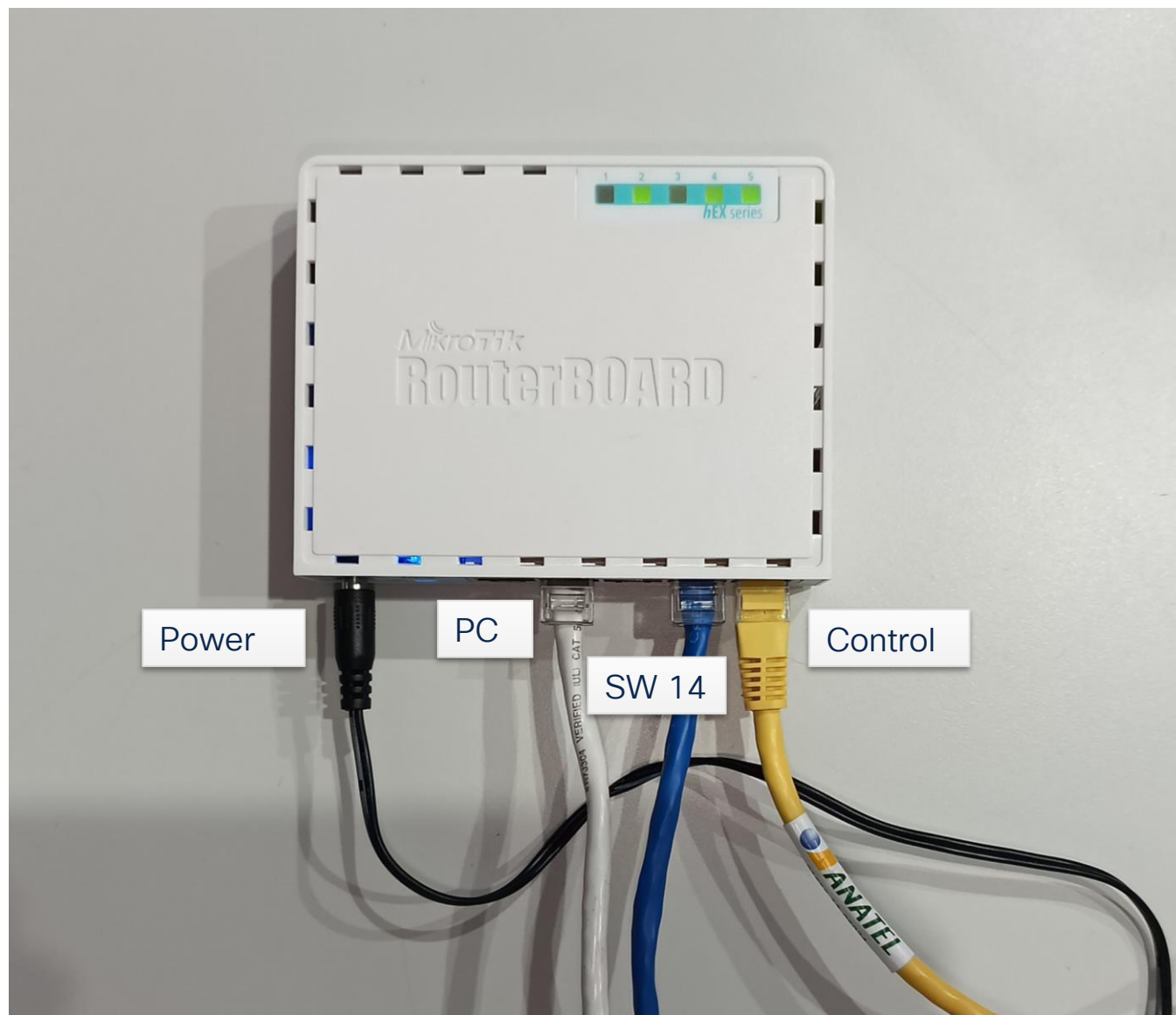


Com um estabilizador de energia

Estabilizador de energia invade redes

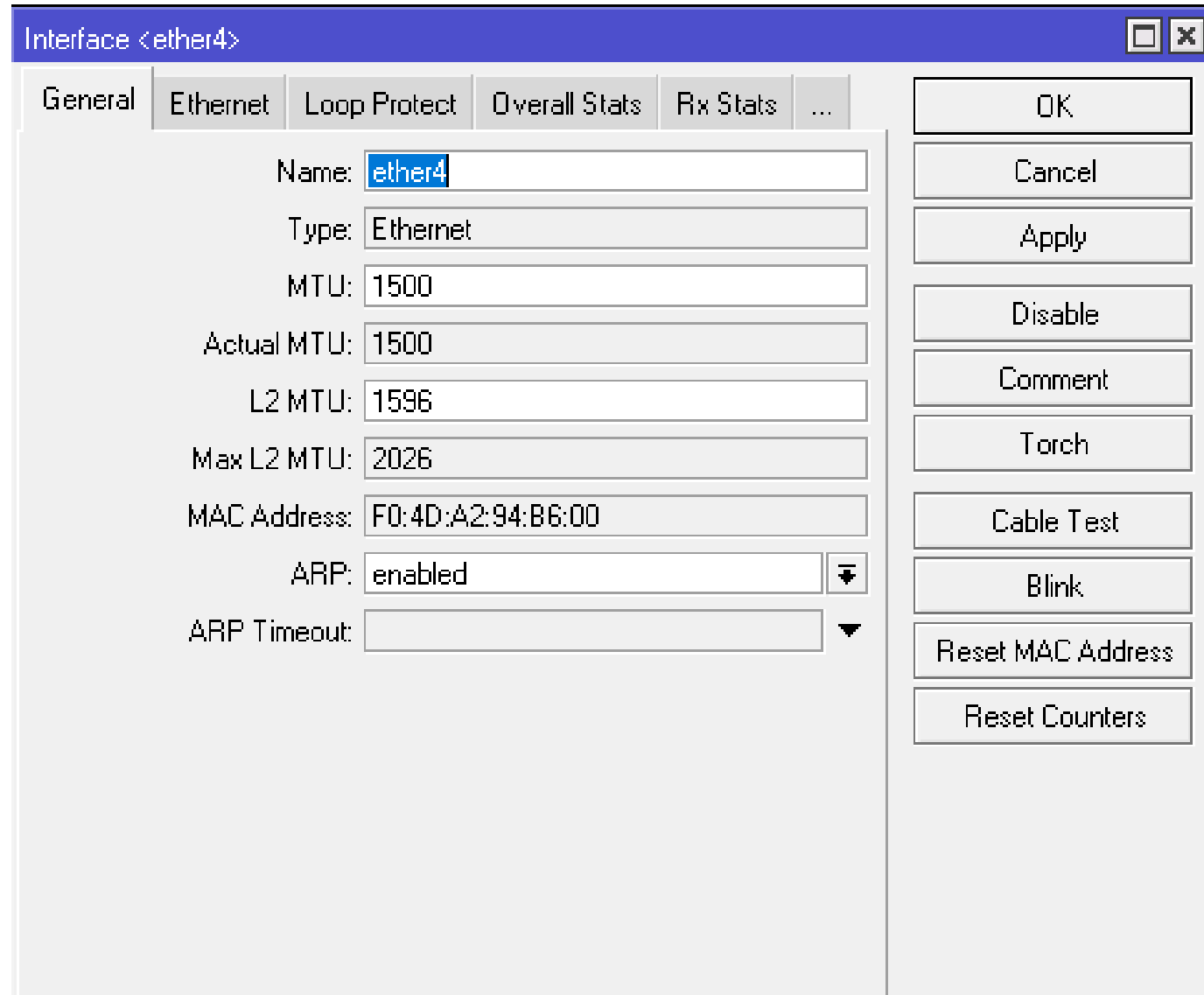
# Mikrotik

Para desempenhar o papel de um dispositivo externo colocado entre o switch e o dispositivo, foi usado um Mikrotik RouterBOARD, que interrompe o link destinado ao endhost e é controlado externamente por um usuário não atento na rede.



# MAC Address Spoofing

O board Mikrotik tem a capacidade de descobrir e re-apropriar para suas interfaces, o endereço MAC do endhost. Depois de executar essa ação, é possível inserir pacotes na comunicação se passando pelo computador afetado.



The screenshot shows the Mikrotik WinBox configuration window for the 'ether4' interface. The window has a blue title bar with the text 'Interface <ether4>' and standard window controls. Below the title bar are several tabs: 'General', 'Ethernet', 'Loop Protect', 'Overall Stats', 'Rx Stats', and an ellipsis. The 'General' tab is selected. The configuration fields are as follows:

- Name: ether4
- Type: Ethernet
- MTU: 1500
- Actual MTU: 1500
- L2 MTU: 1596
- Max L2 MTU: 2026
- MAC Address: F0:4D:A2:94:B6:00
- ARP: enabled (with a dropdown arrow)
- ARP Timeout: (empty field with a dropdown arrow)

On the right side of the window, there is a vertical stack of buttons: OK, Cancel, Apply, Disable, Comment, Torch, Cable Test, Blink, Reset MAC Address, and Reset Counters.

# 802.1x

Usando apenas 802.1x, é possível que o dispositivo invasivo acesse a rede e seus recursos.

The screenshot shows a Cisco Ping utility window with the following configuration:

- General tab selected
- Ping To: 10.0.135.1
- Interface: bridge1
- ARP Ping:
- Packet Count: (empty)
- Timeout: 1000 ms

Buttons on the right: Start, Stop, Close, New Window.

Seq #	Host	Time	Reply Size	Status
102	10.0.135.1	1ms	50	
103	10.0.135.1	0ms	50	
104	10.0.135.1	0ms	50	
105	10.0.135.1	2ms	50	
106	10.0.135.1	1ms	50	
107	10.0.135.1	1ms	50	
108	10.0.135.1	1ms	50	
109	10.0.135.1	1ms	50	
110	10.0.135.1	1ms	50	
111	10.0.135.1	1ms	50	
112	10.0.135.1	1ms	50	
113	10.0.135.1	1ms	50	
114	10.0.135.1	1ms	50	
115	10.0.135.1	1ms	50	
116	10.0.135.1	1ms	50	
117	10.0.135.1	1ms	50	
118	10.0.135.1	1ms	50	
119	10.0.135.1	0ms	50	
120	10.0.135.1	1ms	50	

Summary: 121 items | 121 of 121 packets... | 0% packet loss | Min: 0 ms | Avg: 1 ms | Max: 26 ms

# MACSec

Depois de mudar para o perfil MACSec, não é mais possível interagir com a rede de forma significativa para o invasor.

The screenshot shows the Cisco IOS 'Ping' utility window. The 'Advanced' tab is selected, displaying the following configuration:

- Ping To: 10.0.135.1
- Interface: bridge1
- ARP Ping
- Packet Count: (empty)
- Timeout: 1000 ms

On the right side, there are buttons for 'Start', 'Stop', 'Close', and 'New Window'. Below the configuration, a table displays the results of the ping attempts:

Seq #	Host	Time	Reply Size	Status
12	10.0.135.1	timeout		timeout
13	10.0.135.1	timeout		timeout
14	127.0.0.1	928ms	78	host unreachable
15	10.0.135.1	timeout		timeout
16	10.0.135.1	timeout		timeout
17	127.0.0.1	899ms	78	host unreachable
18	10.0.135.1	timeout		timeout
19	10.0.135.1	timeout		timeout
20	127.0.0.1	932ms	78	host unreachable
21	10.0.135.1	timeout		timeout
22	10.0.135.1	timeout		timeout
23	127.0.0.1	859ms	78	host unreachable
24	10.0.135.1	timeout		timeout
25	10.0.135.1	timeout		timeout
26	127.0.0.1	894ms	78	host unreachable
27	10.0.135.1	timeout		timeout
28	10.0.135.1	timeout		timeout
29	127.0.0.1	848ms	78	host unreachable
30	10.0.135.1	timeout		timeout
31	10.0.135.1	timeout		timeout

At the bottom of the window, a summary bar indicates: 32 items, 0 of 32 packets received, 100% packet loss.

# Referências

- Guia de configuração MACsec e MKA:  
<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/macsec/configuration/xe-16/macsec-xe-16-book/wan-macsec-mka-support-Enhance.html>
- 802.1AE MACsec White Paper:  
<https://www.cisco.com/c/dam/en/us/td/docs/solutions/Enterprise/Security/MACsec/WP-High-Speed-WAN-Encrypt-MACsec.pdf>
- Innovations in Ethernet Encryption  
<https://www.cisco.com/c/dam/en/us/td/docs/solutions/Enterprise/Security/MACsec/WP-High-Speed-WAN-Encrypt-MACsec.pdf>

Muito Obrigado  
por acompanhar a sessão

e boa quinta!