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

Quinta às Quinze 21/03/2024

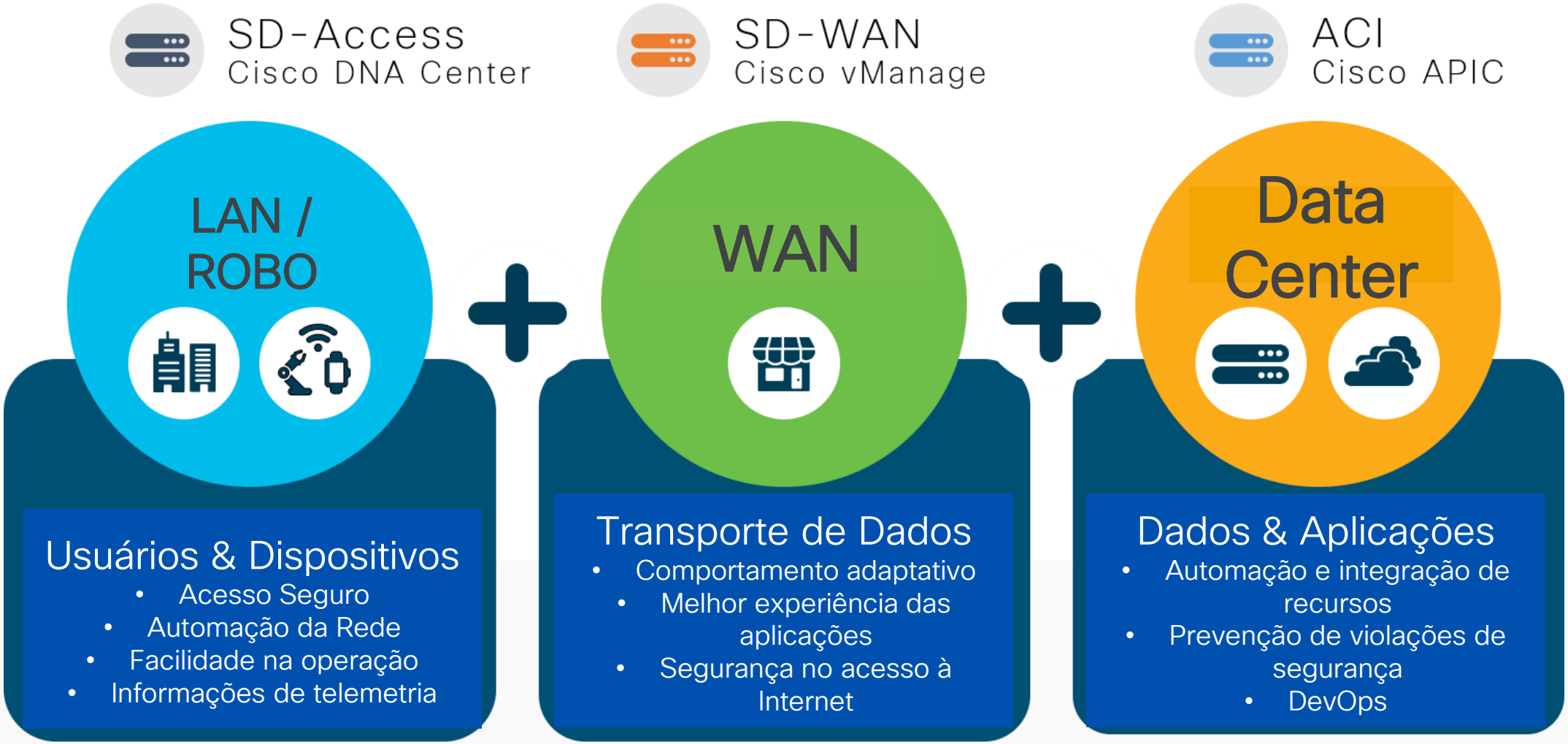
Elvio de Sousa linkedin.com/in/elvio-net-br

Engineer @ Cisco | Msc | ITQ | 5x CCNP

Gabriel Almeida linkedin.com/in/gabriel-tollendal/

Engineer @ Cisco | CCNA

Laboratório de Transferência Tecnológica (LTT)
Visão de sua arquitetura



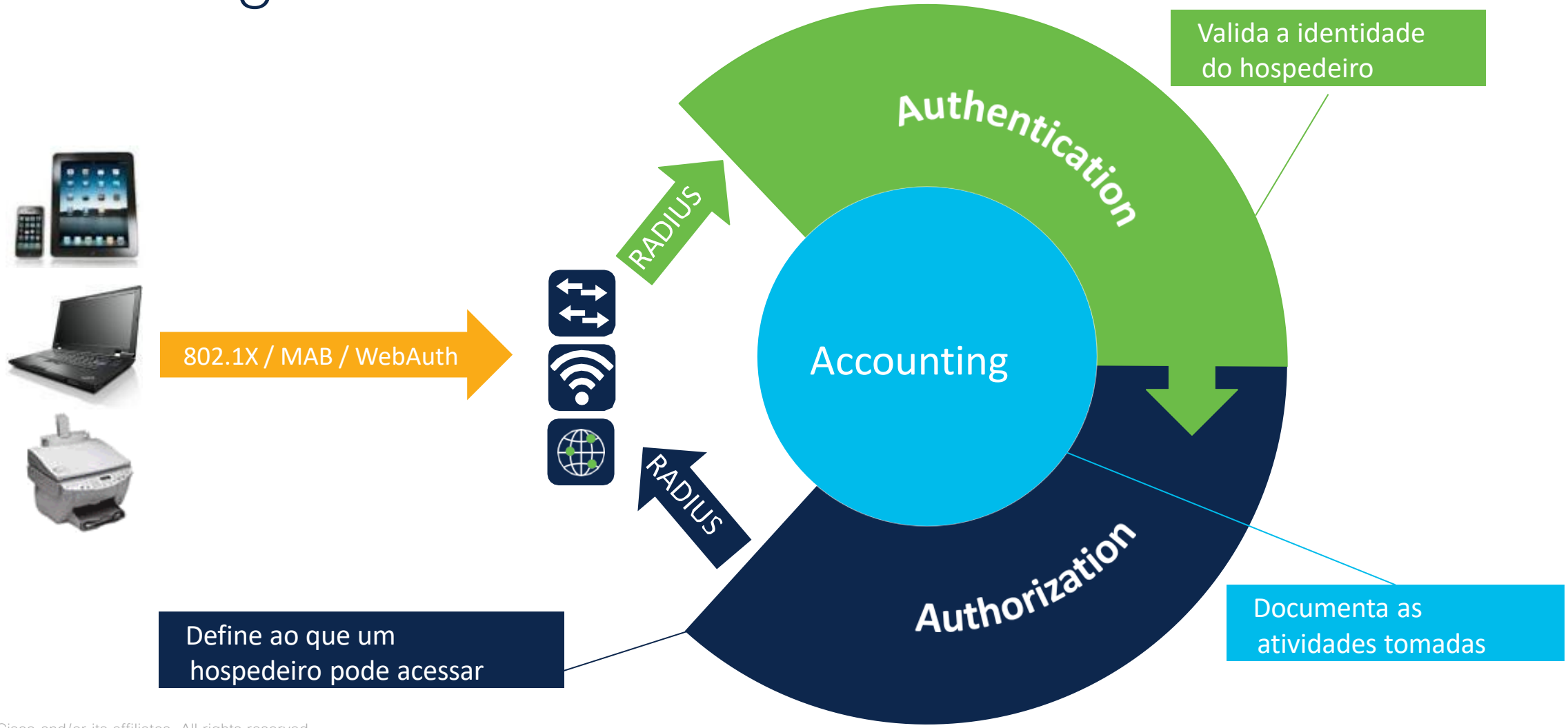
Outras soluções: MERAKI, Segurança, AppDynamics, ThousandEyes, etc.

AGENDA

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

Fundamentos de AAA

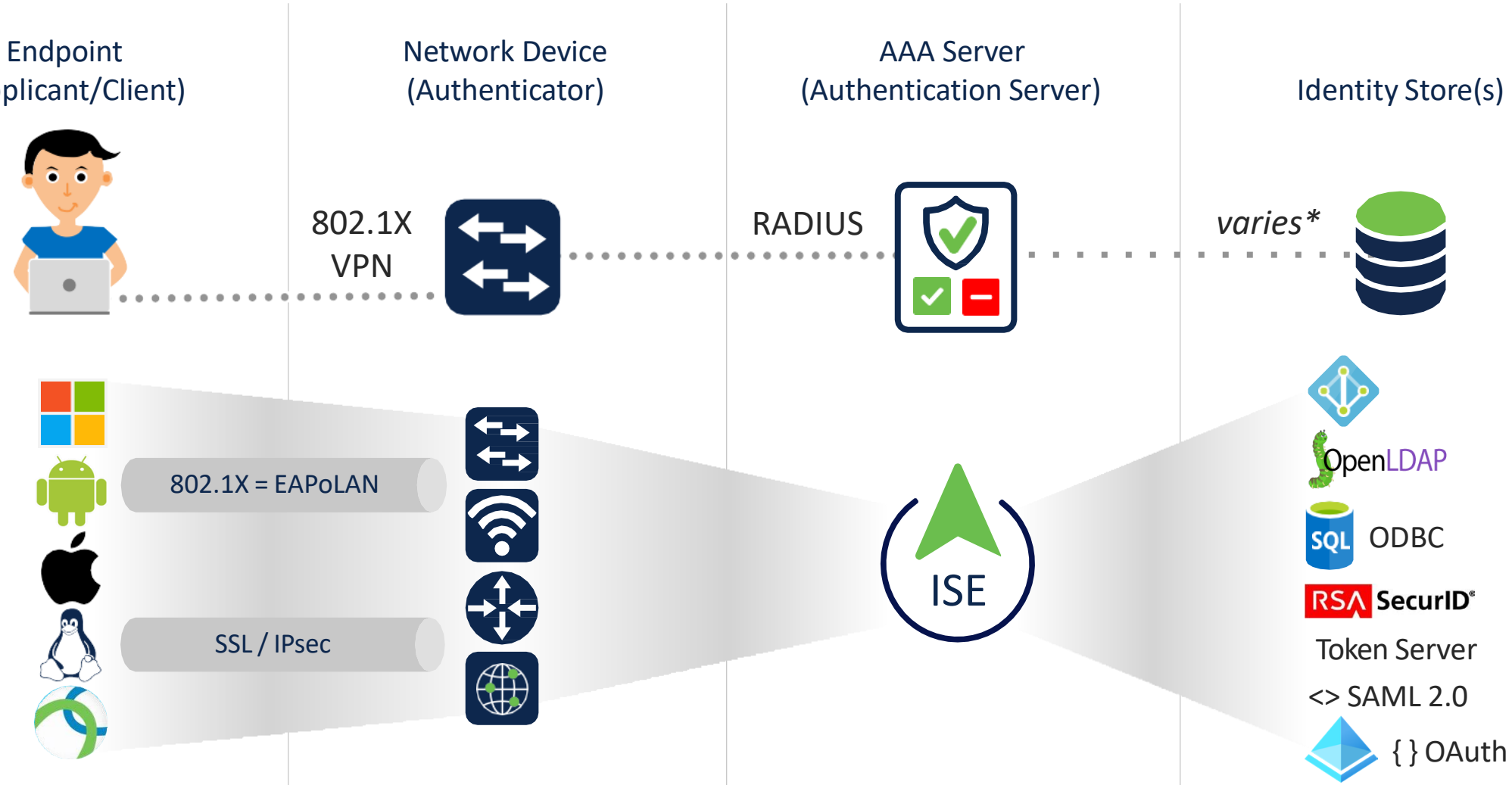
Authentication, Authorization and Accounting



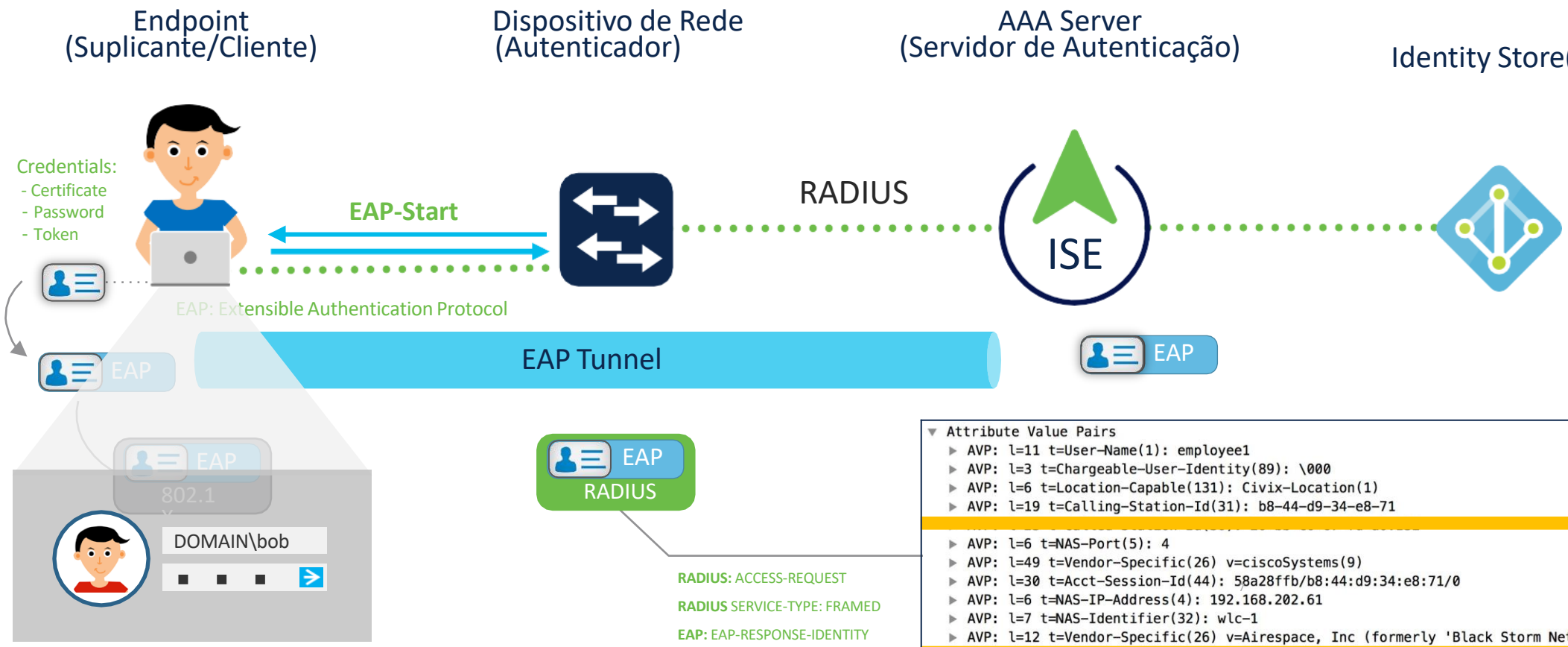
Operação de um Servidor RADIUS

RADIUS = Remote Authentication Dial-In User Service

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

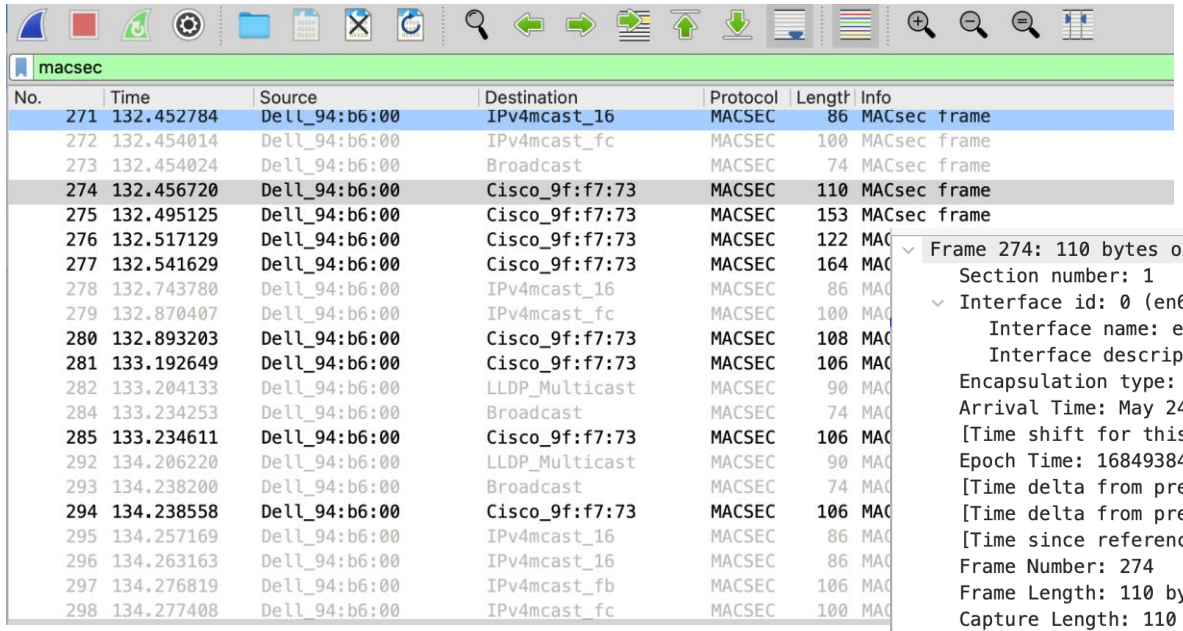


Fundamentos IEEE 802.1X



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



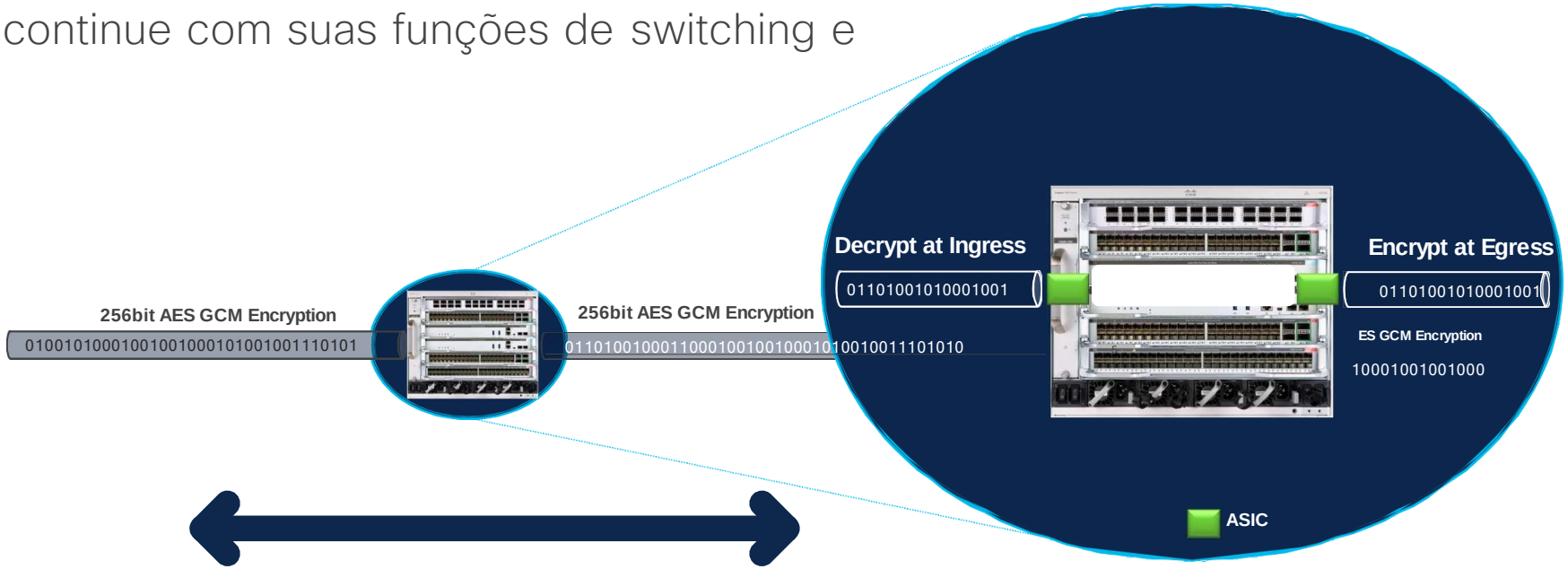
- Captura pacotes 802.1AE

```
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]
```

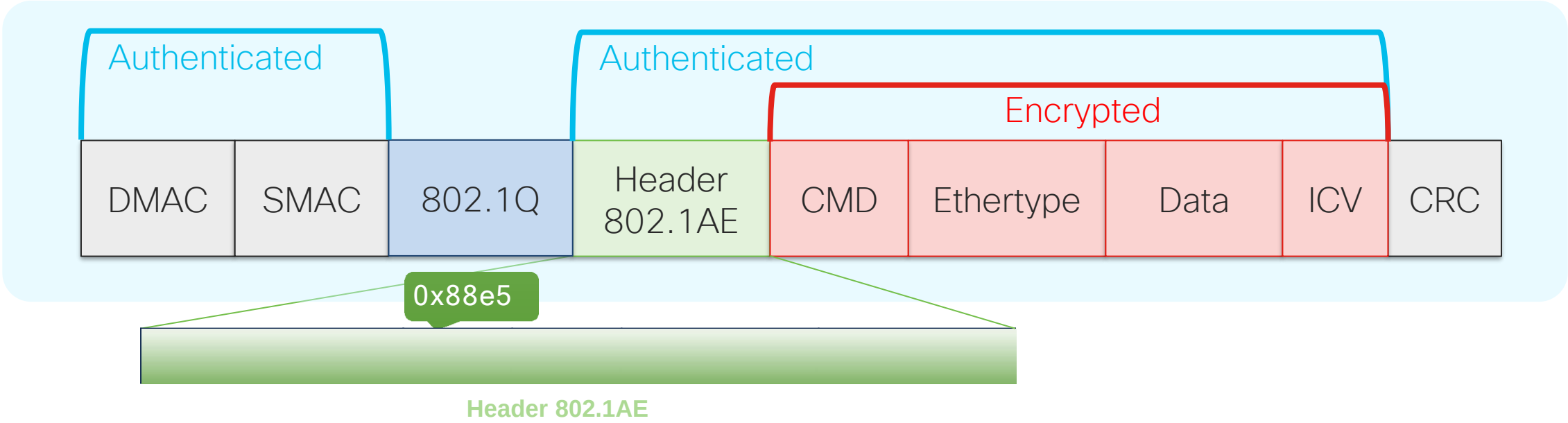
Resumidamente,

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

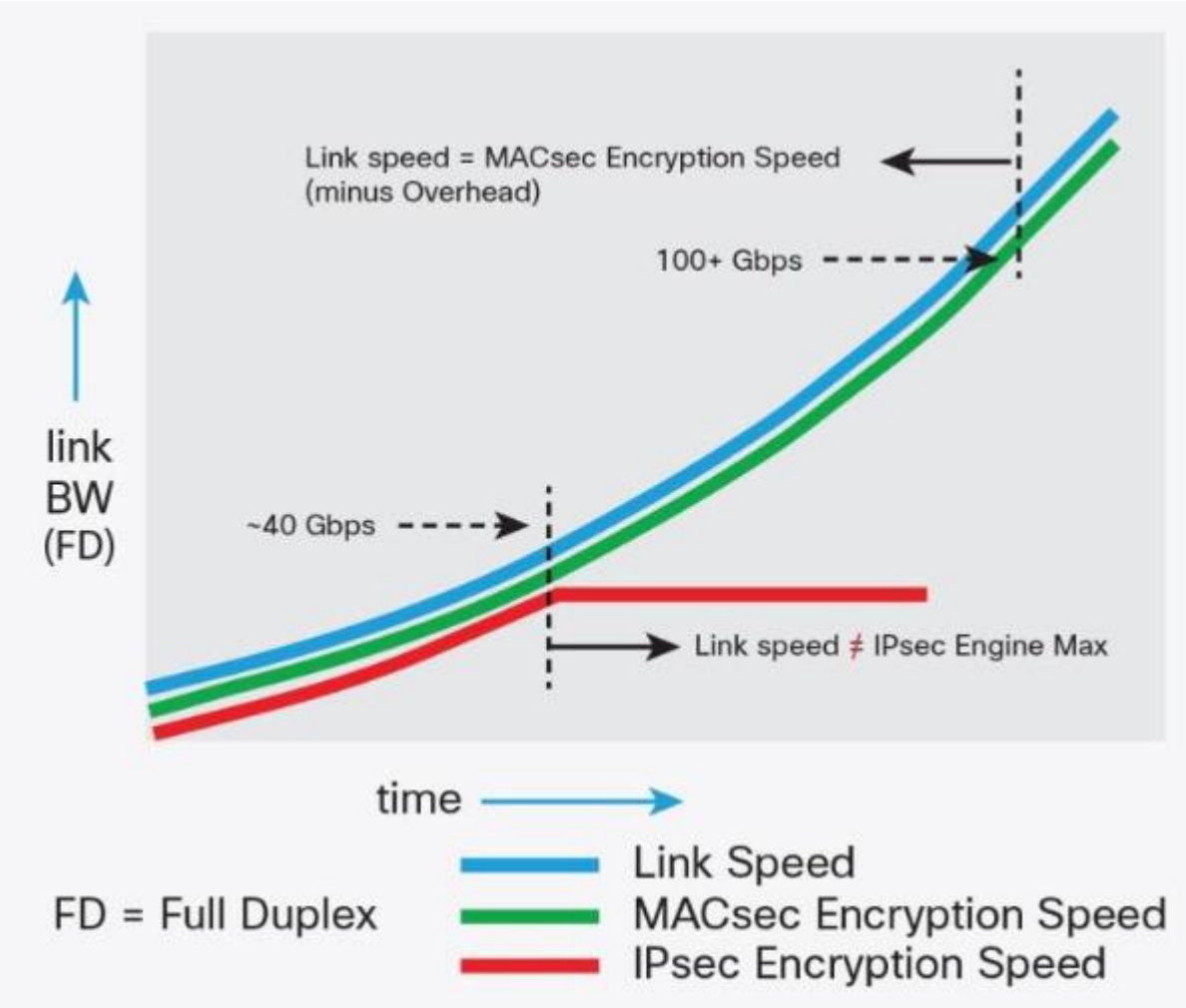


Estrutura de um Frame 802.1AE para LAN



- 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

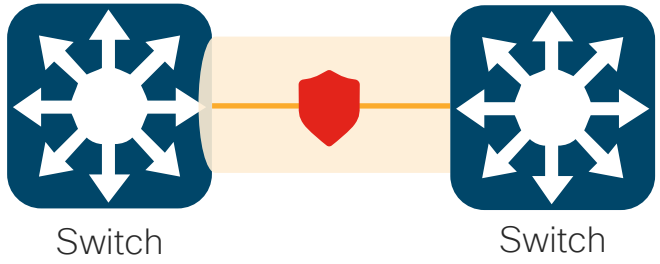


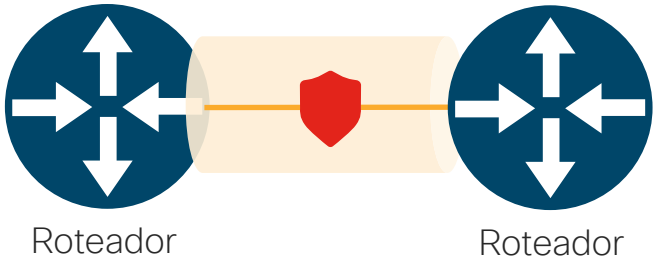
- Se uma implementação exigir que todo o tráfego que sai/passa pelo roteador precisa ser criptografado, a taxa de transferência do roteador agora será restrita ao desempenho do mecanismo IPsec.

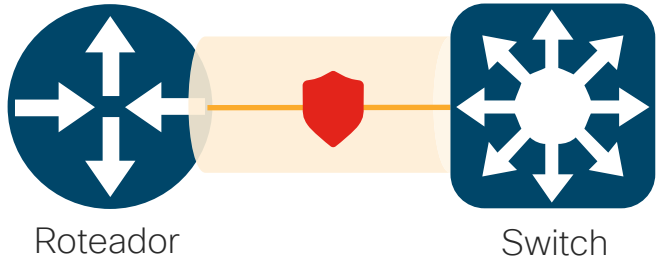
- MACsec, como o nome indica, é a criptografia da camada MAC e oferece criptografia igual à das taxas de porta Ethernet (1/10/40) bidireccionalmente, independentemente do tamanho do pacote tamanho do pacote, executando a função de criptografia na camada física (PHY) da porta Ethernet.

LAN MACsec

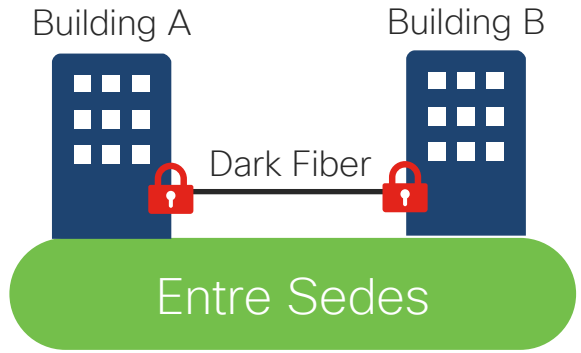
Encripta todo o trafego após o header 802.1Q



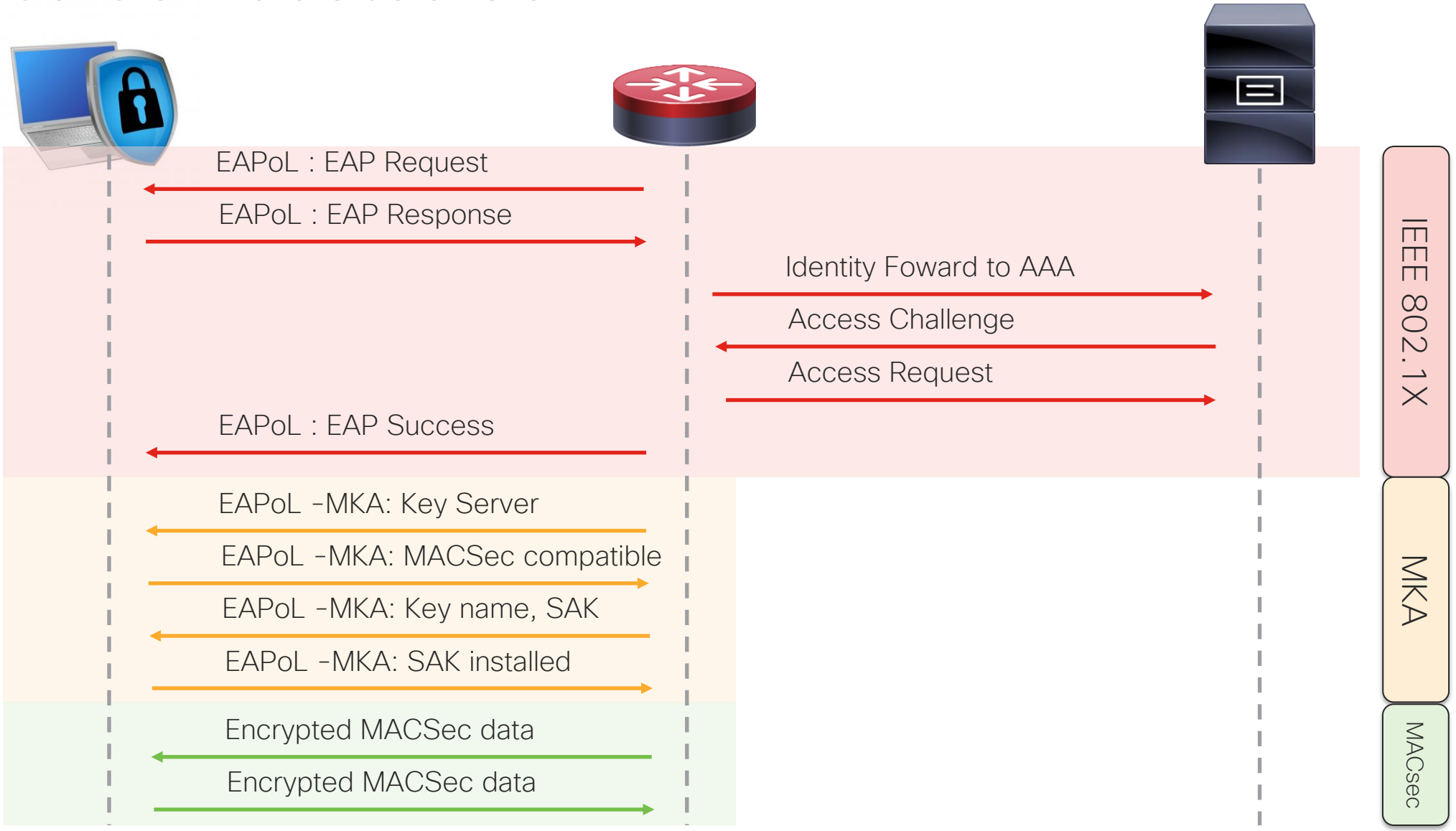




Onde podemos usar o LAN MACsec?



Troca de Pacotes 802.1AE



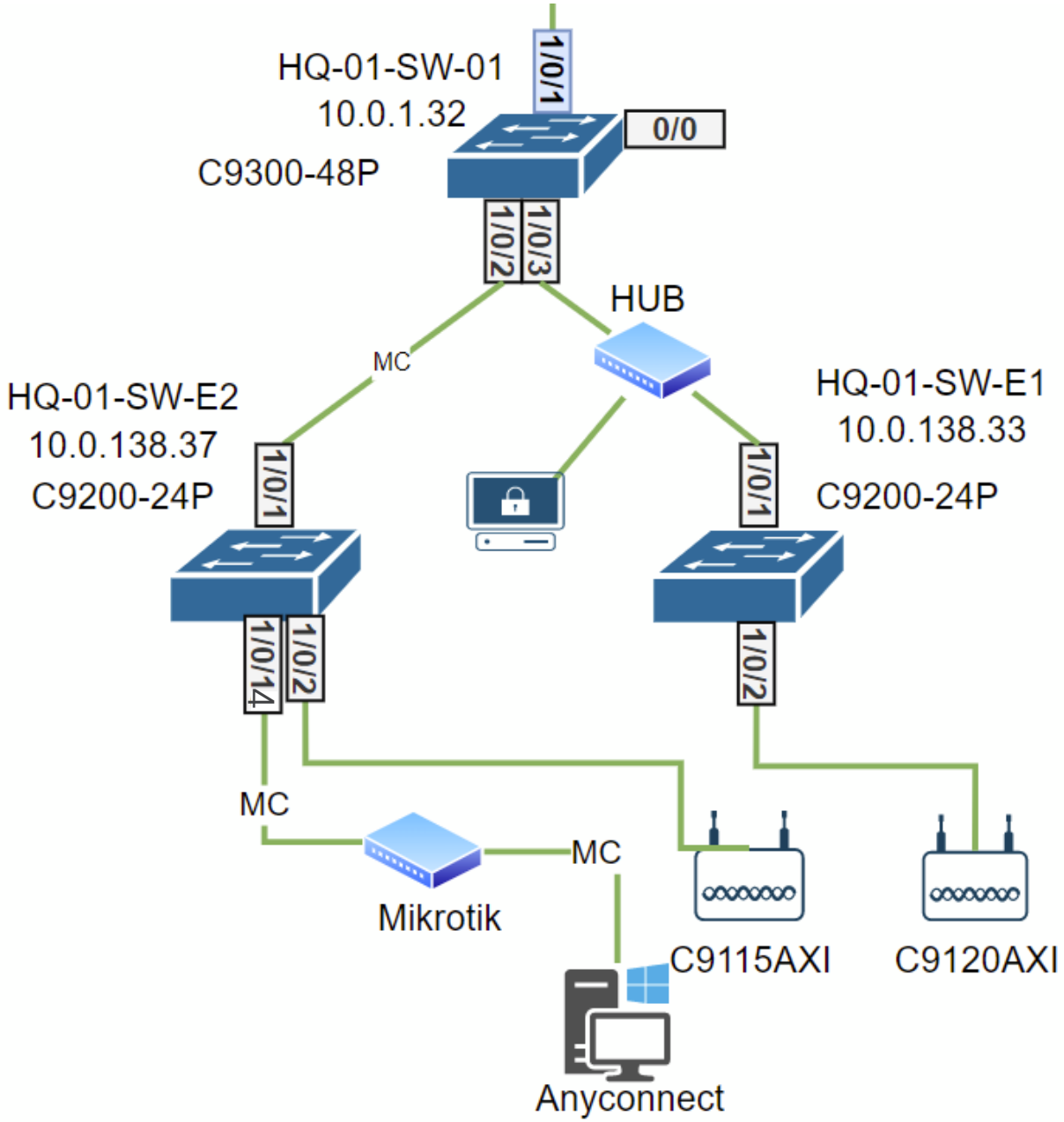
Comaração MACSec com IPSec

	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	Linerate (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	Linerate (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

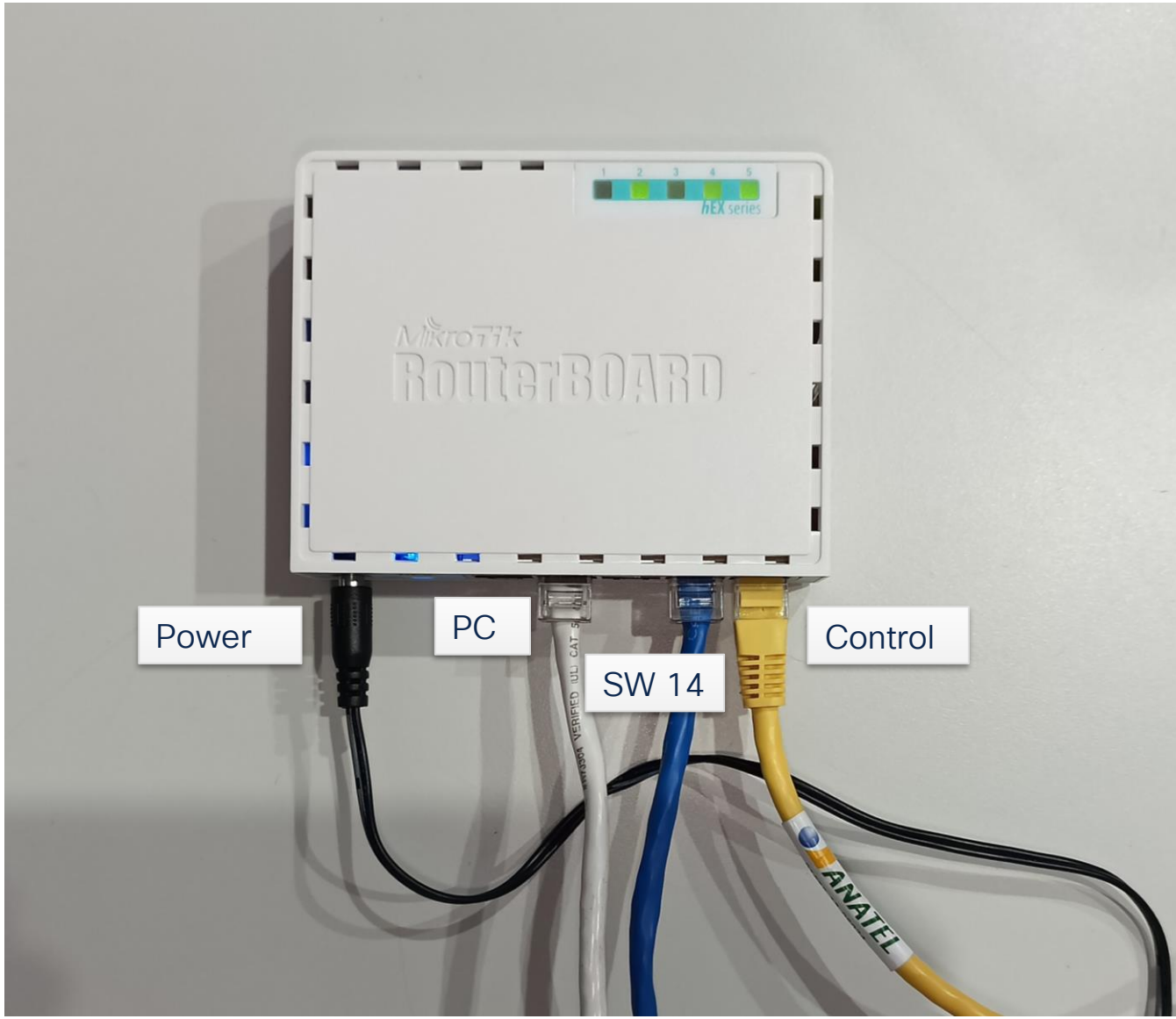
Topologia



Exemplo do Ataque

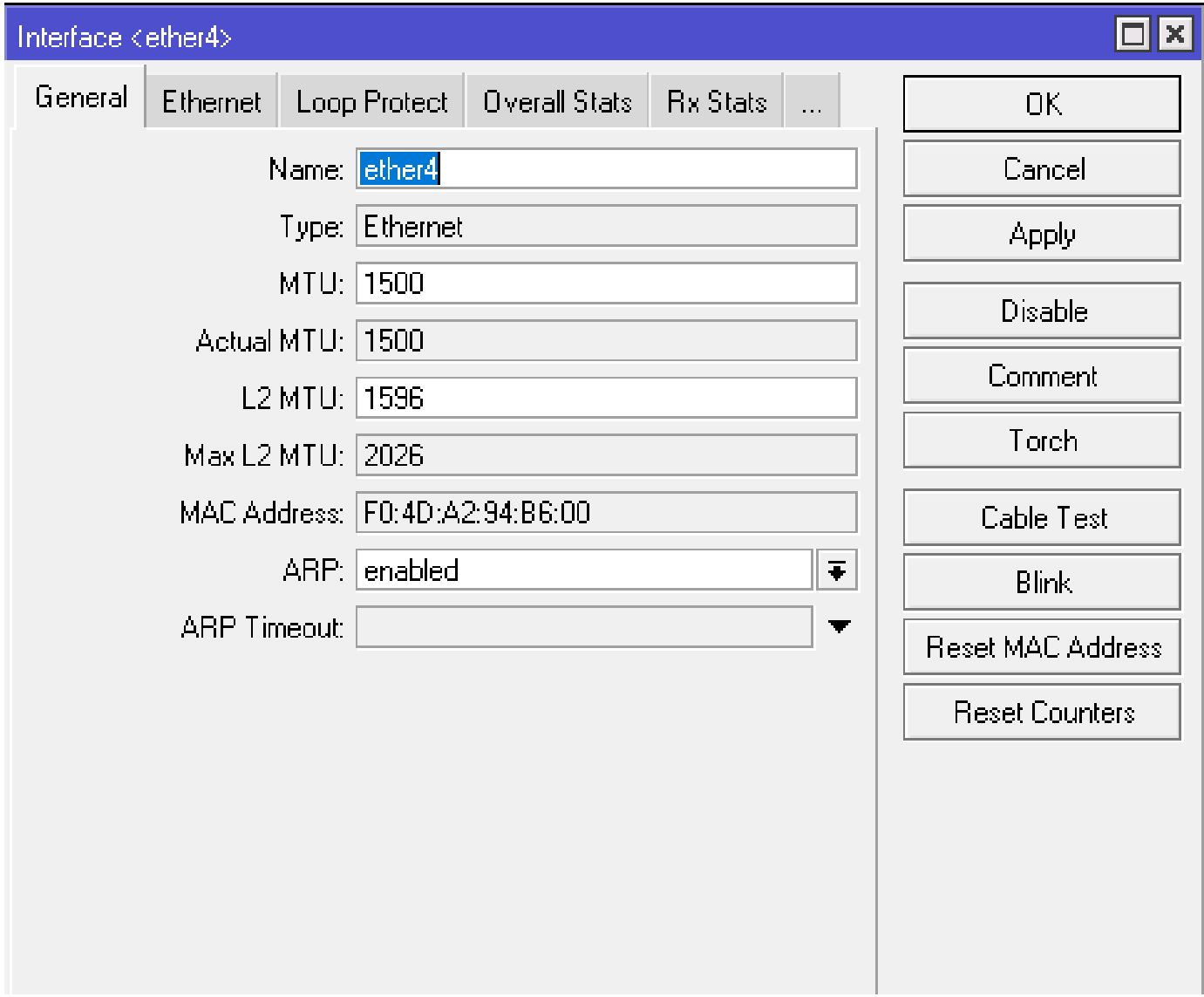
Mikrotik

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.



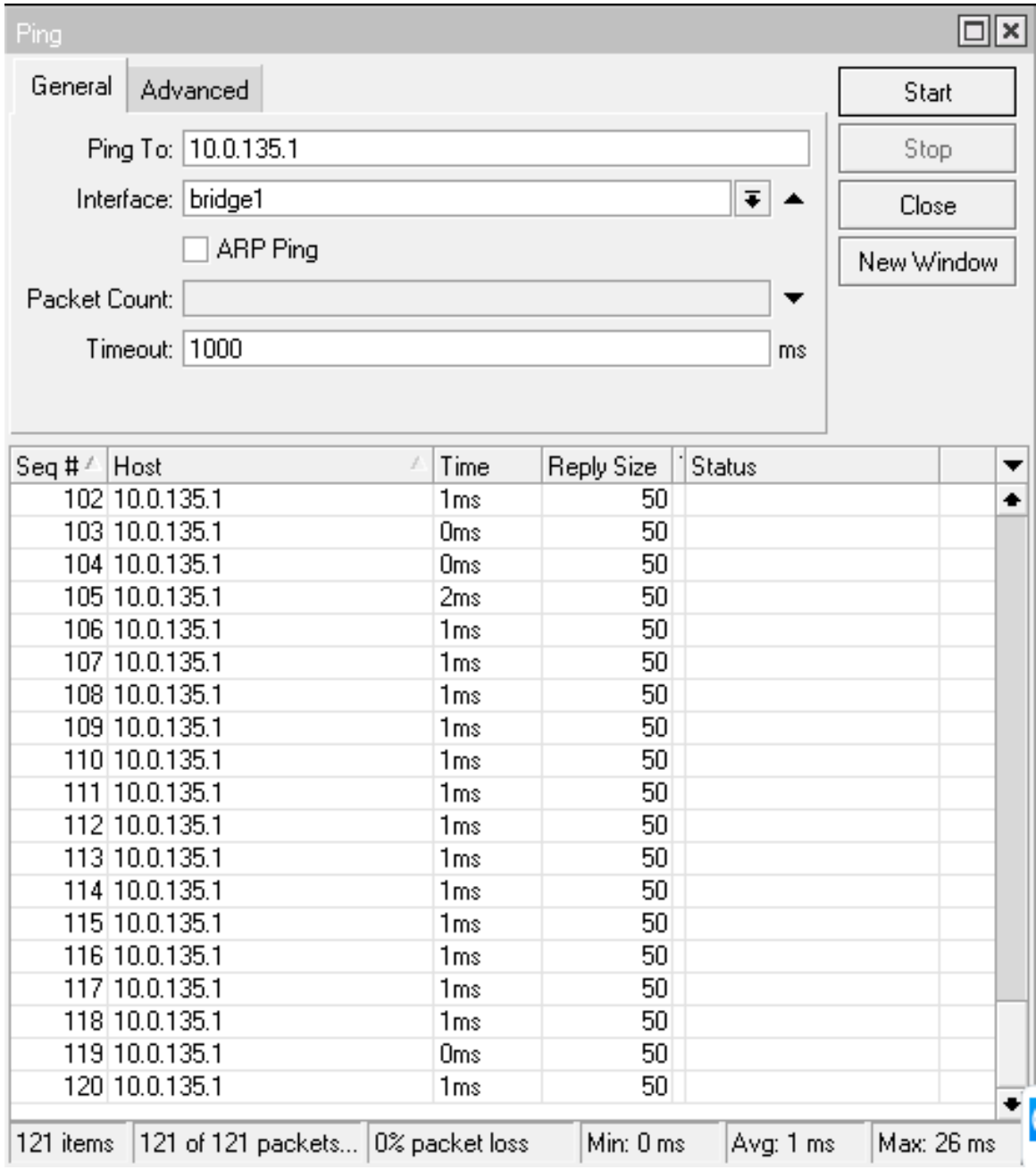
MAC Address Spoofing

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.



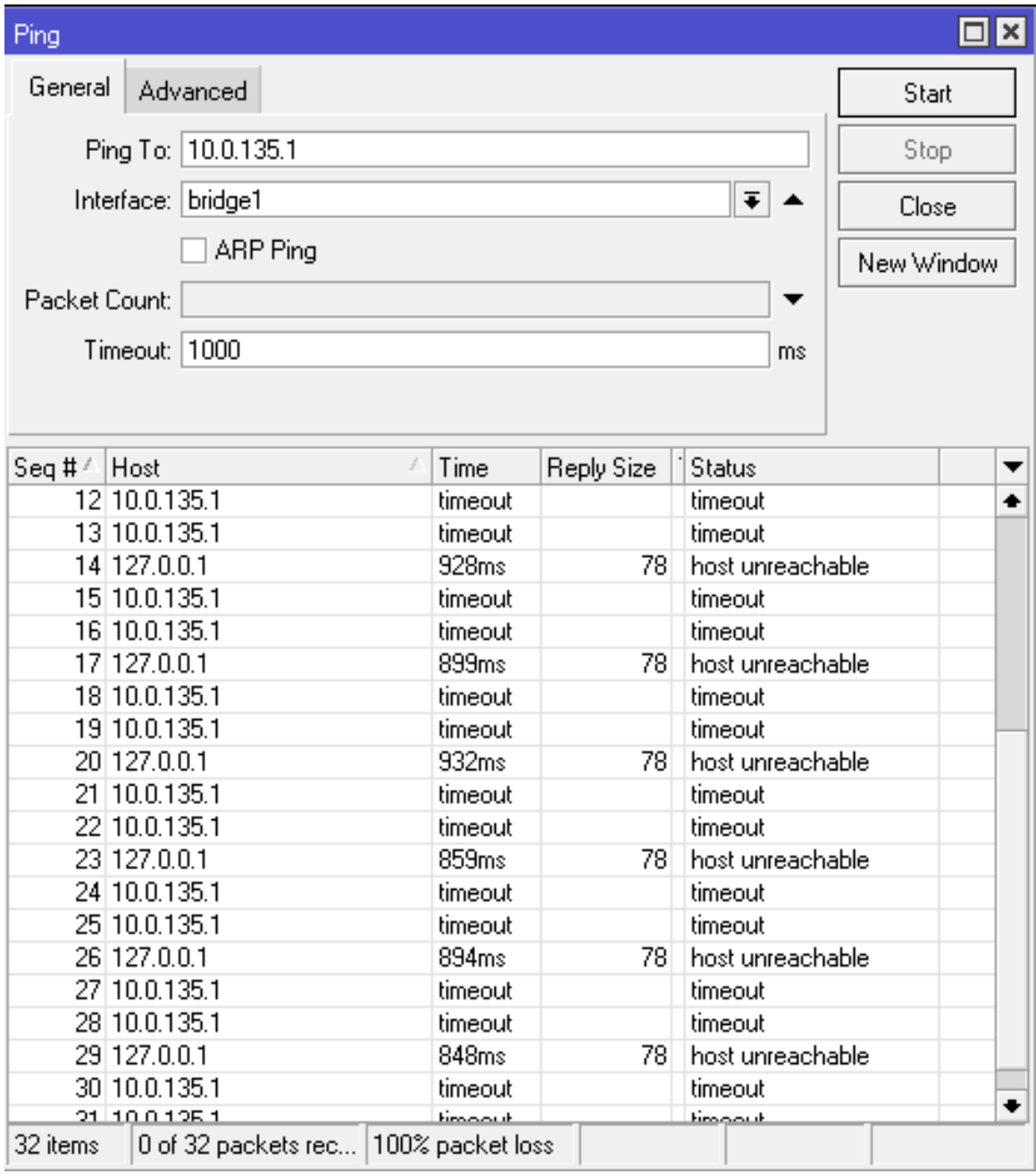
802.1x

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



MACSec

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



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!