Uso do MacSec (802.1ae) em complemento ao 802.1x em redes corporativas

Controle de admissão e proteção man-in-the-middle

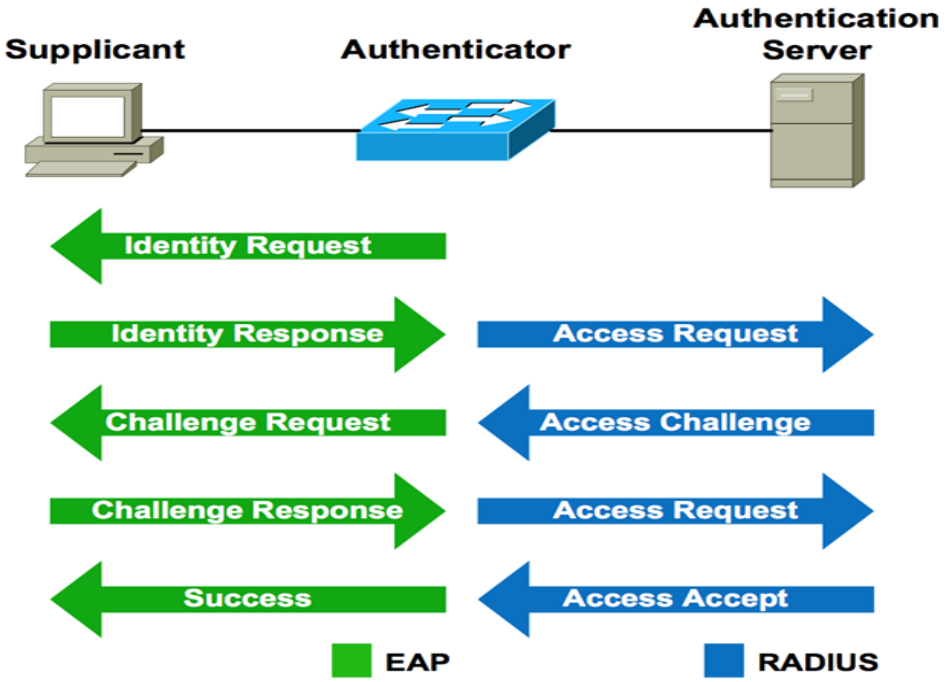
Wilson Rogério Lopes

LACNIC 27 / GTS 29

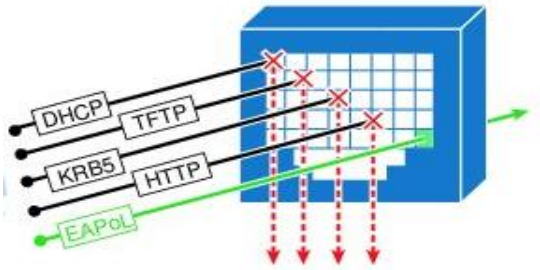
05/2017

IEEE 802.1x

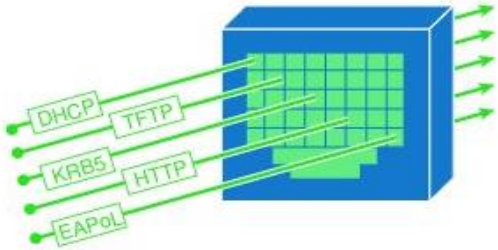
- Primeiro padrão - 802.1X-2001, update 802.1X-2004
- Fornece mecanismo de autenticação para LAN
- EAPoL (EAP over LAN)
- 3 entidades – Suplicante, Autenticador, Servidor de Autenticação



Porta não autorizada

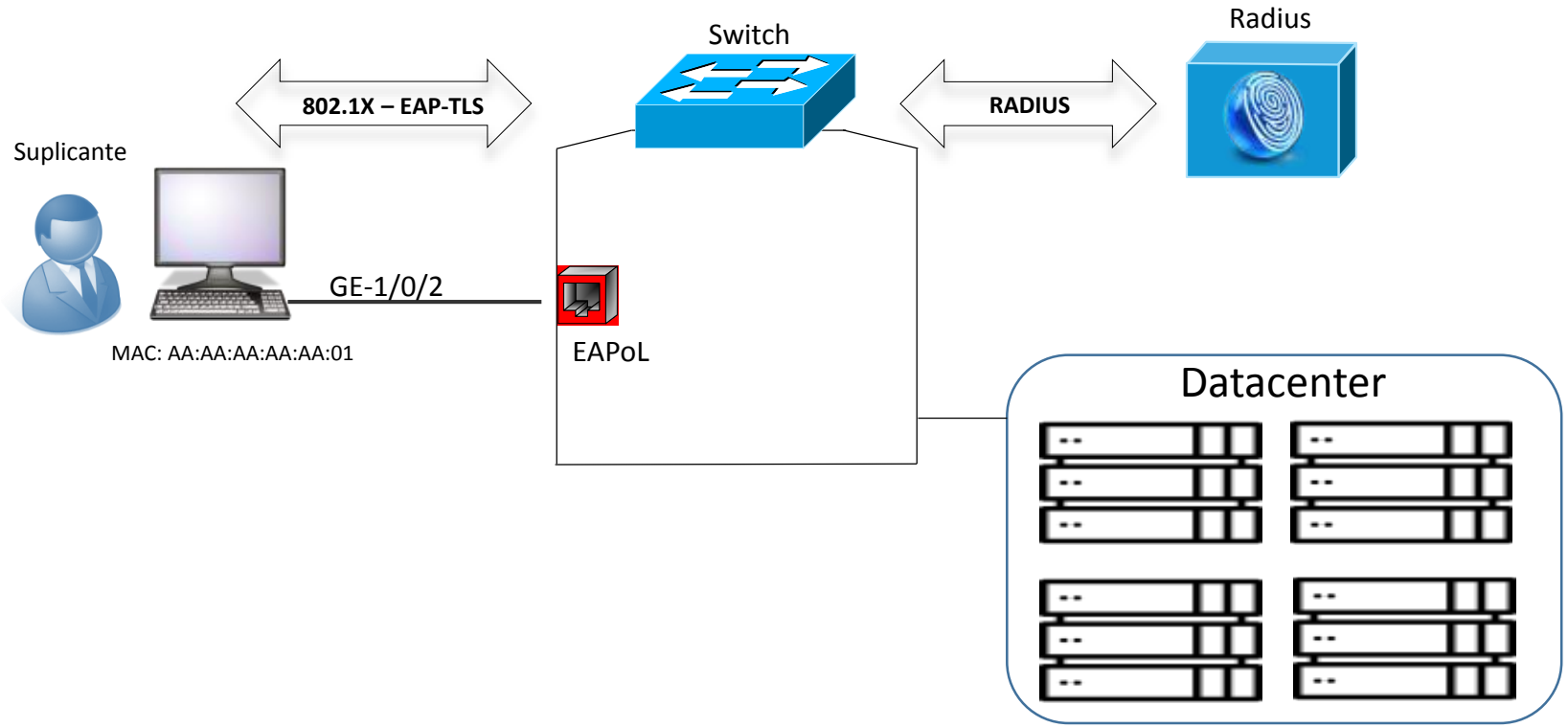


Porta autorizada



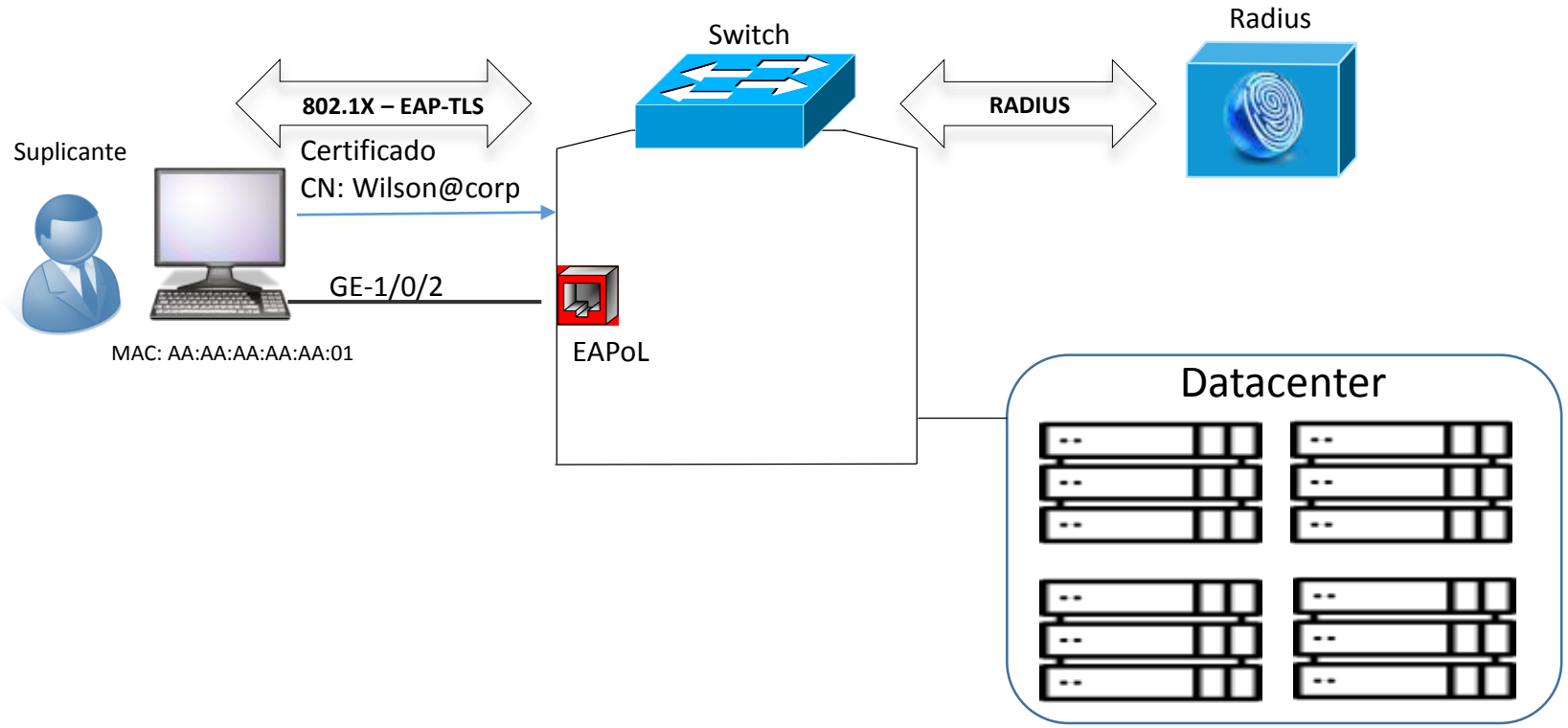
IEEE 802.1x

- Endpoint Autenticado = mac-address autorizado
- Tráfego permitido até queda do link ou re-autenticação periódica



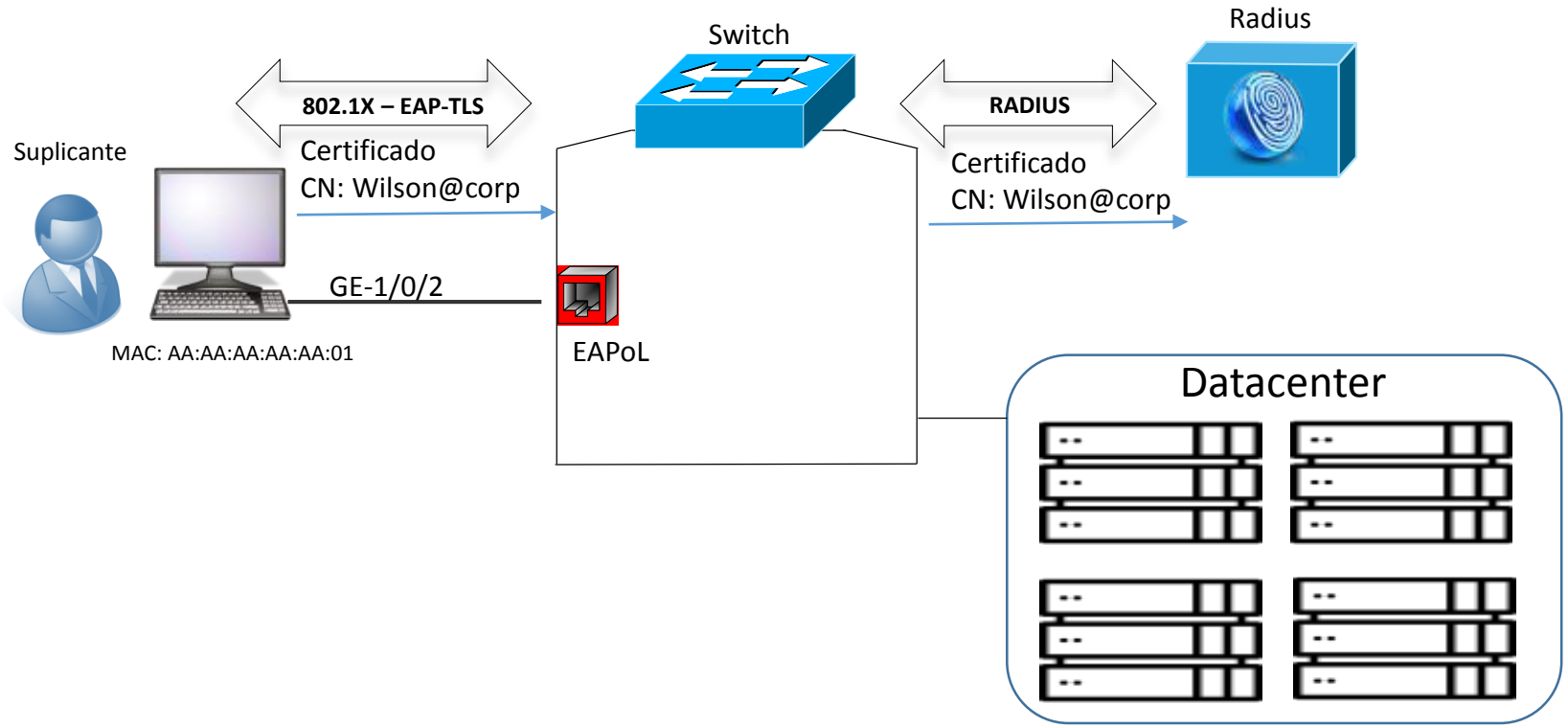
IEEE 802.1x

- Endpoint Autenticado = mac-address autorizado
- Tráfego permitido até queda do link ou re-autenticação periódica



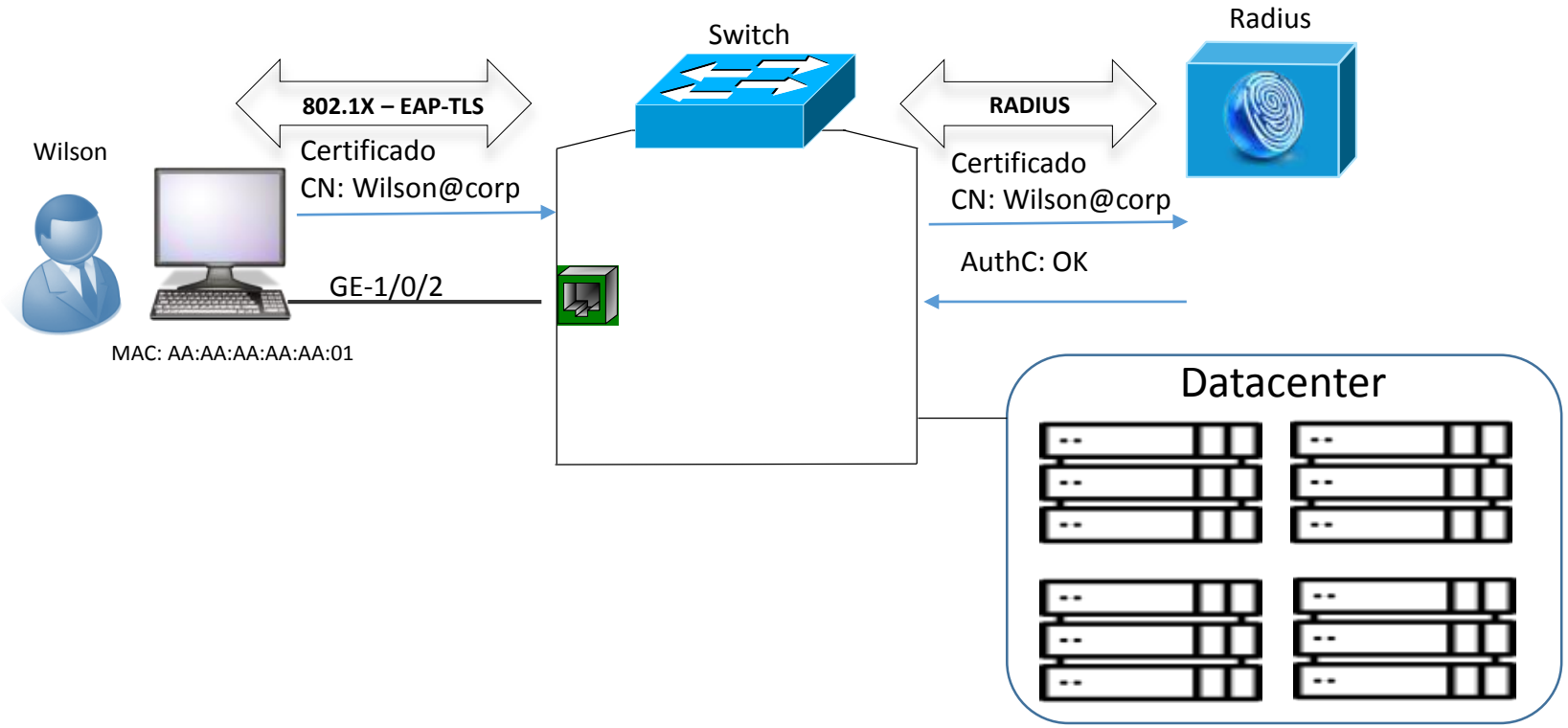
IEEE 802.1x

- Endpoint Autenticado = mac-address autorizado
- Tráfego permitido até queda do link ou re-autenticação periódica



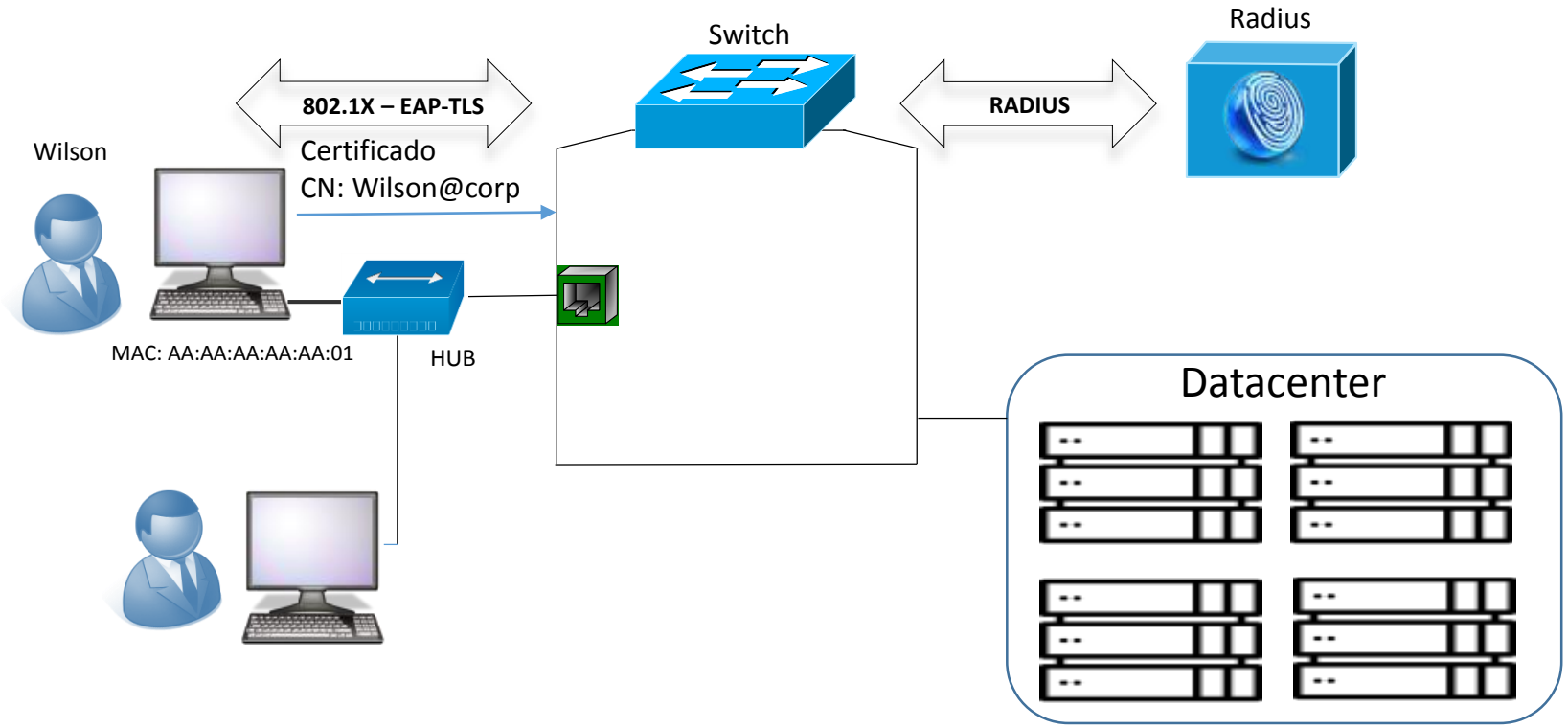
IEEE 802.1x

- Endpoint Autenticado = mac-address autorizado
- Tráfego permitido até queda do link ou re-autenticação periódica



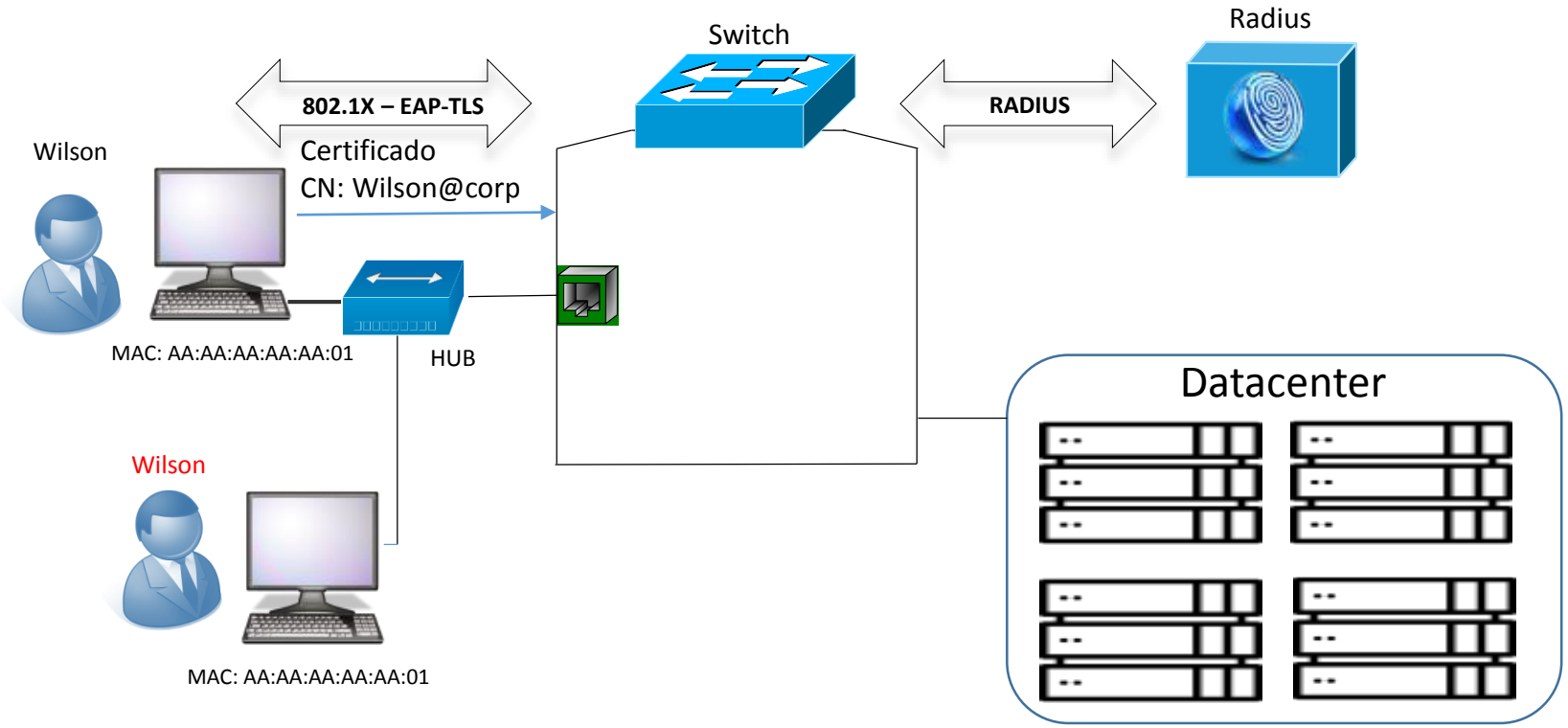
802.1x – Man-in-the-middle

- HUB conectado na porta do switch



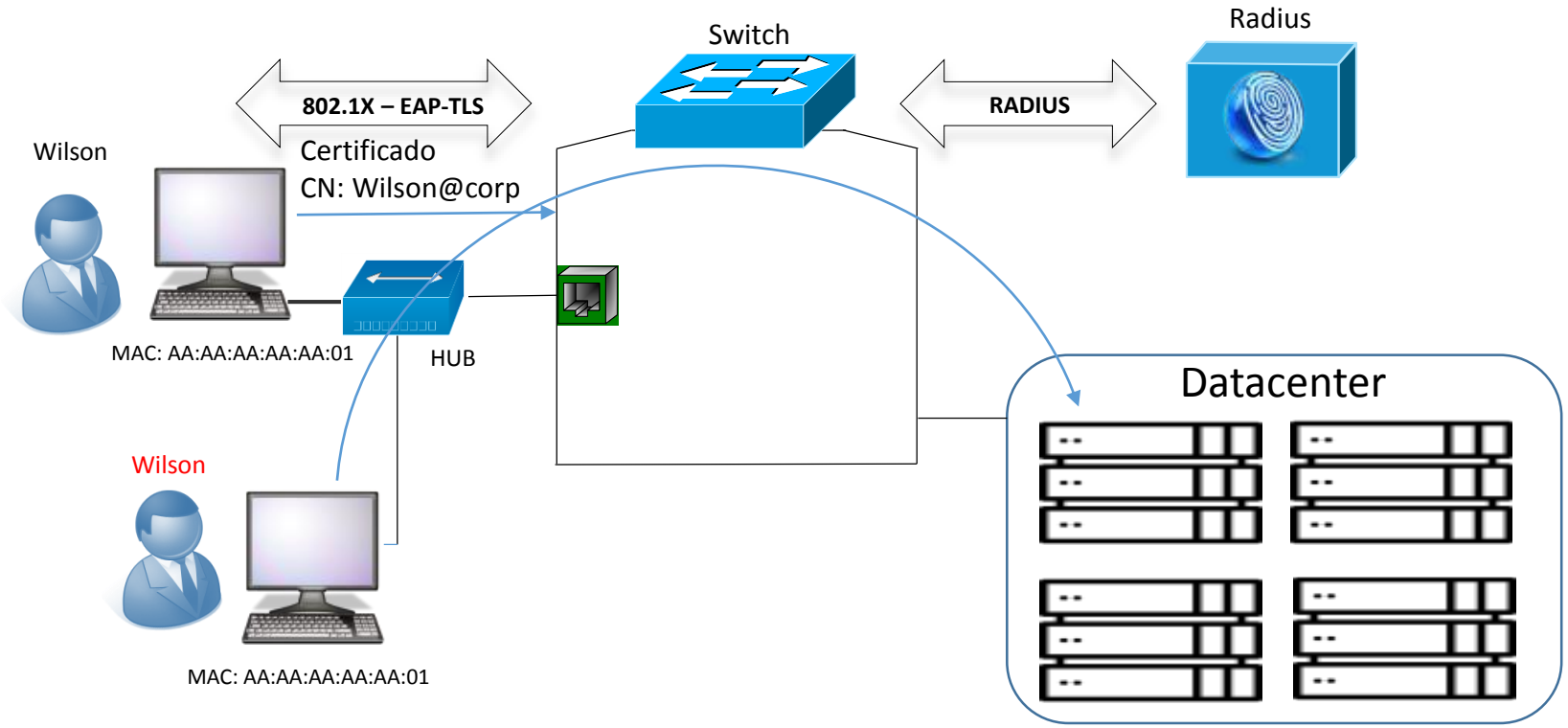
802.1x – Man-in-the-middle

- HUB conectado na porta do switch
- Cliente autenticado
- Mac-address clonado pelo atacante
- Acesso liberado até re-autenticação ou queda do link



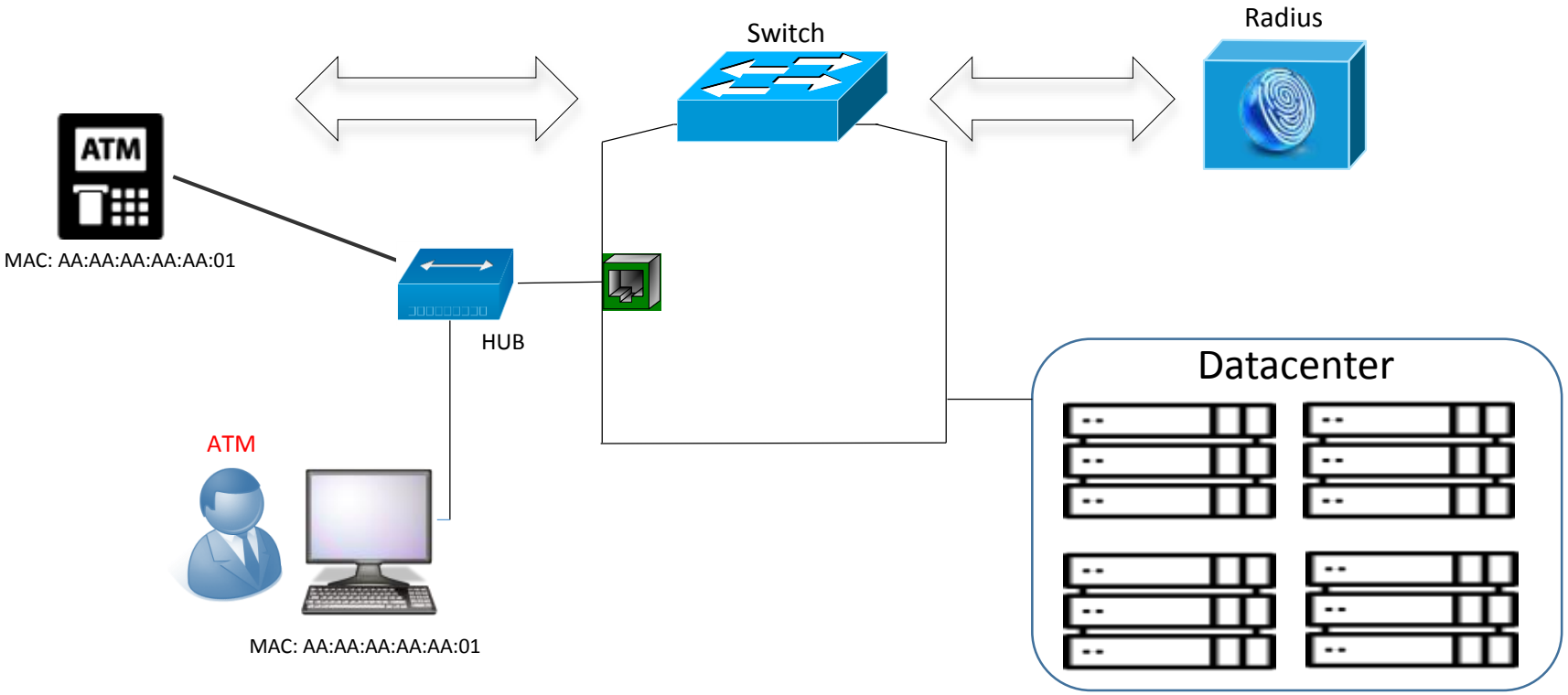
802.1x – Man-in-the-middle

- HUB conectado na porta do switch
- Cliente autenticado
- Mac-address clonado pelo atacante
- Acesso liberado até re-autenticação ou queda do link



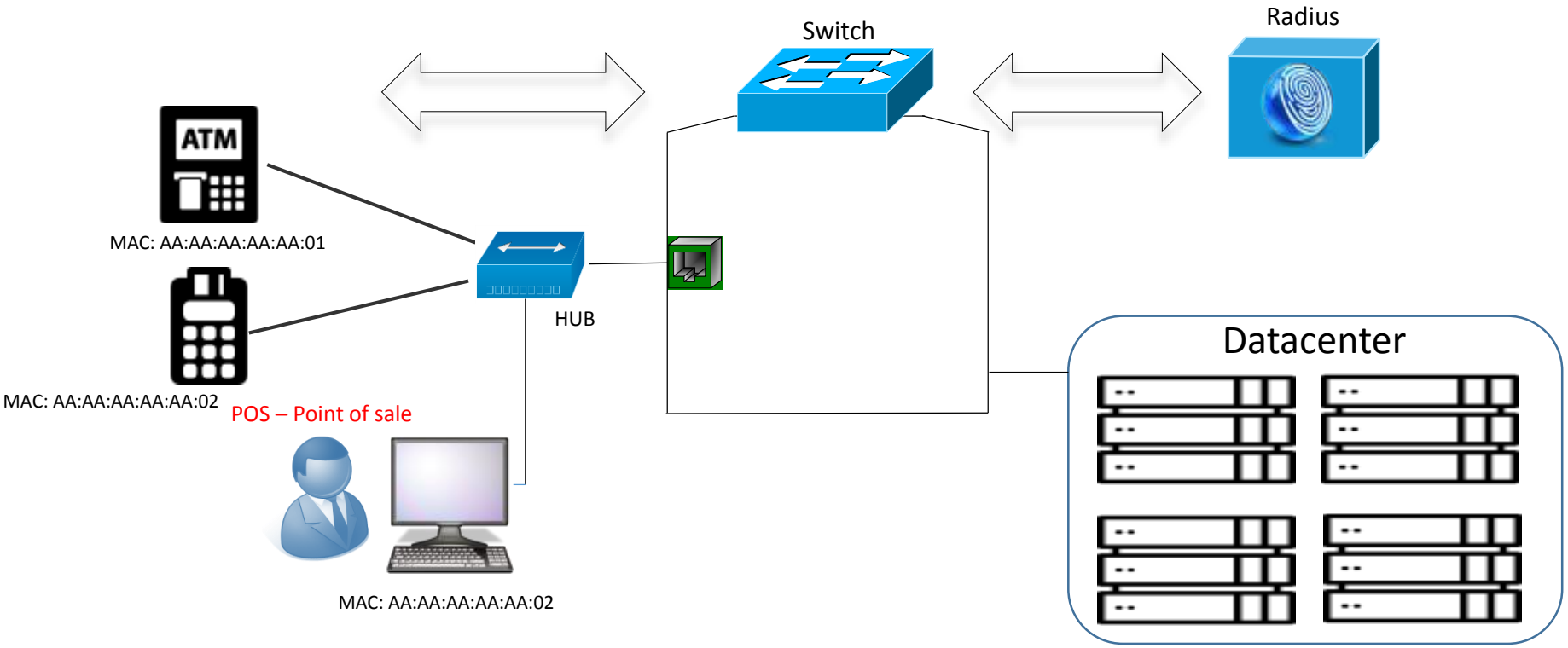
802.1x – Man-in-the-middle

- HUB conectado na porta do switch
- Cliente autenticado
- Mac-address clonado pelo atacante
- Acesso liberado até re-autenticação ou queda do link



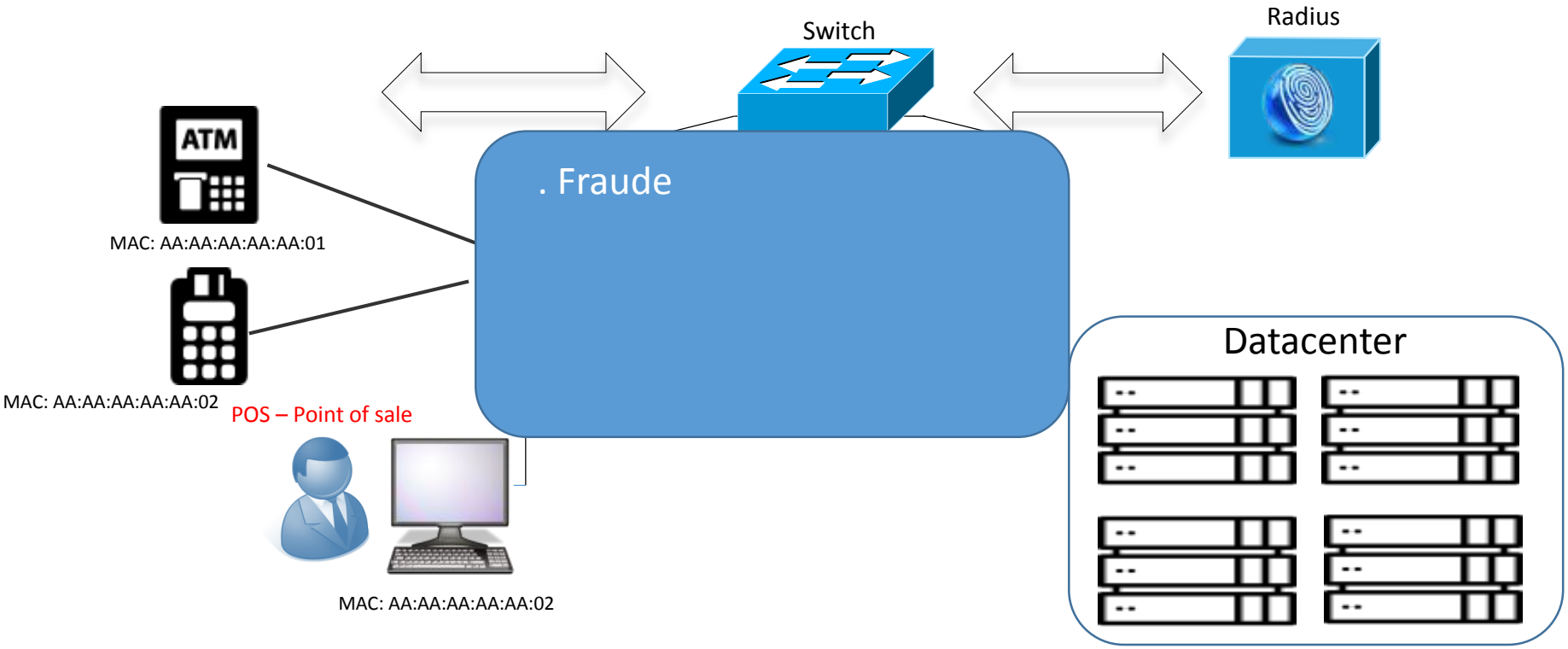
802.1x – Man-in-the-middle

- HUB conectado na porta do switch
- Cliente autenticado
- Mac-address clonado pelo atacante
- Acesso liberado até re-autenticação ou queda do link



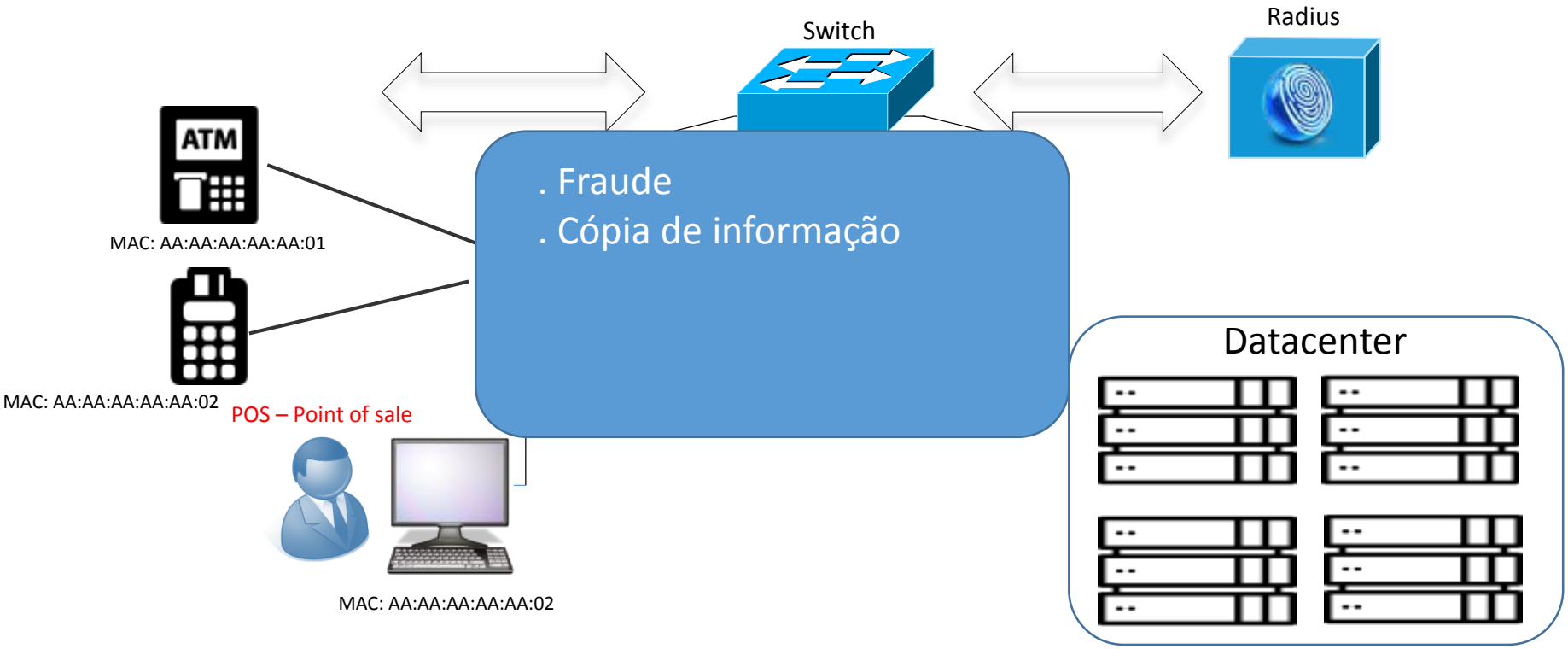
802.1x – Man-in-the-middle

- HUB conectado na porta do switch
- Cliente autenticado
- Mac-address clonado pelo atacante
- Acesso liberado até re-autenticação ou queda do link



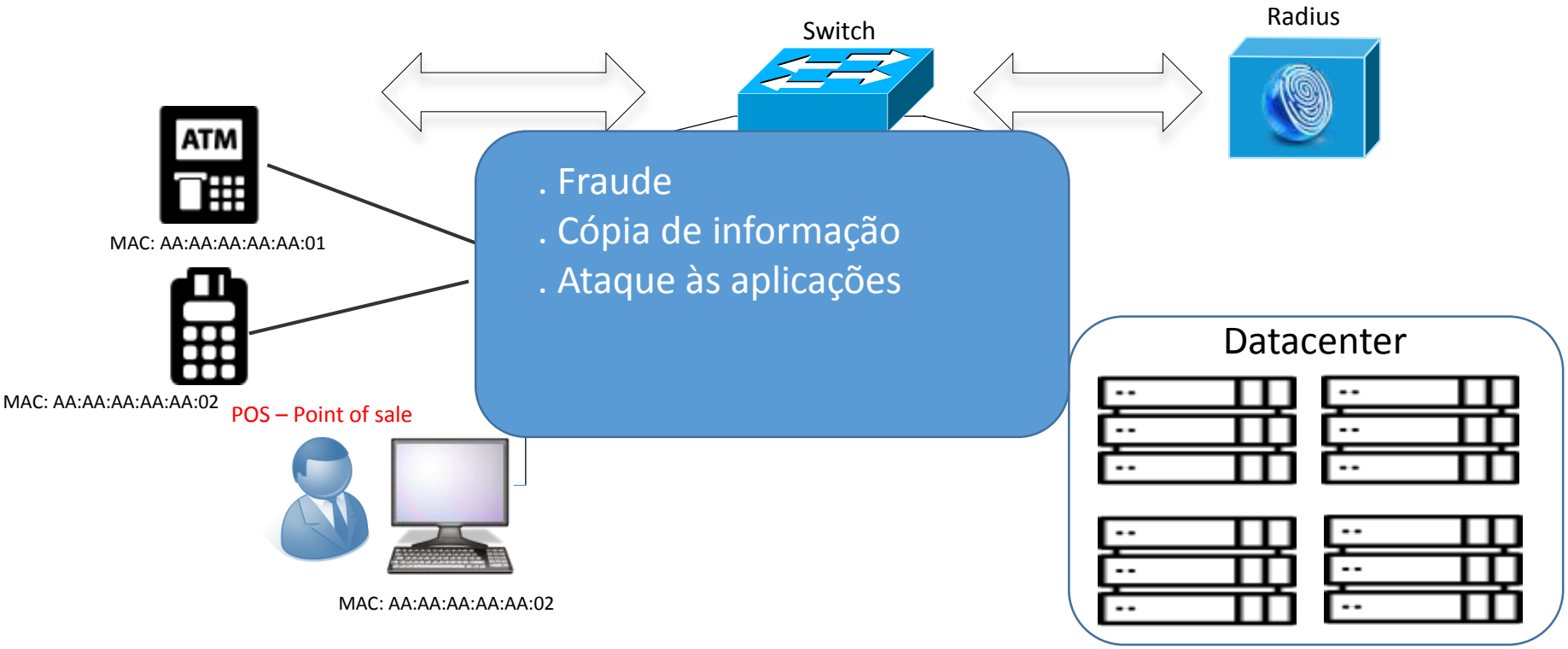
802.1x – Man-in-the-middle

- HUB conectado na porta do switch
- Cliente autenticado
- Mac-address clonado pelo atacante
- Acesso liberado até re-autenticação ou queda do link



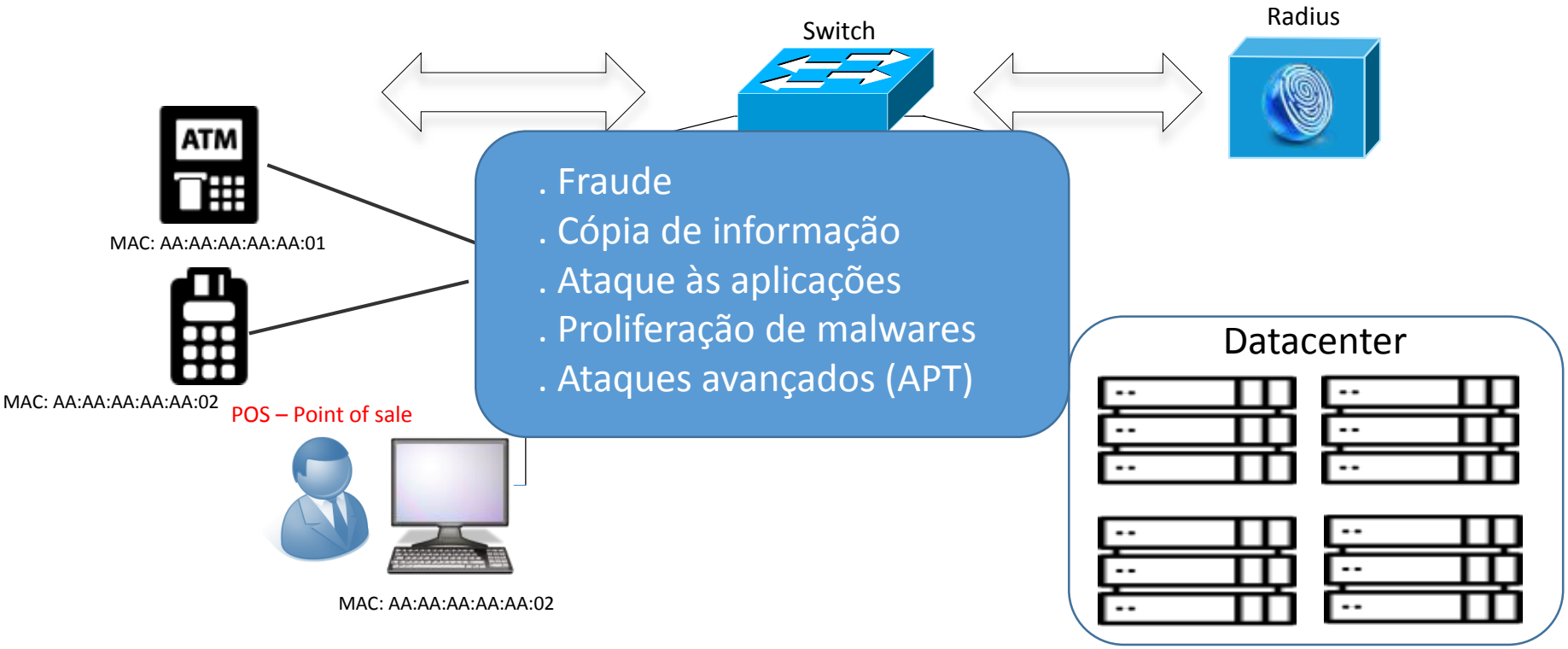
802.1x – Man-in-the-middle

- HUB conectado na porta do switch
- Cliente autenticado
- Mac-address clonado pelo atacante
- Acesso liberado até re-autenticação ou queda do link



802.1x – Man-in-the-middle

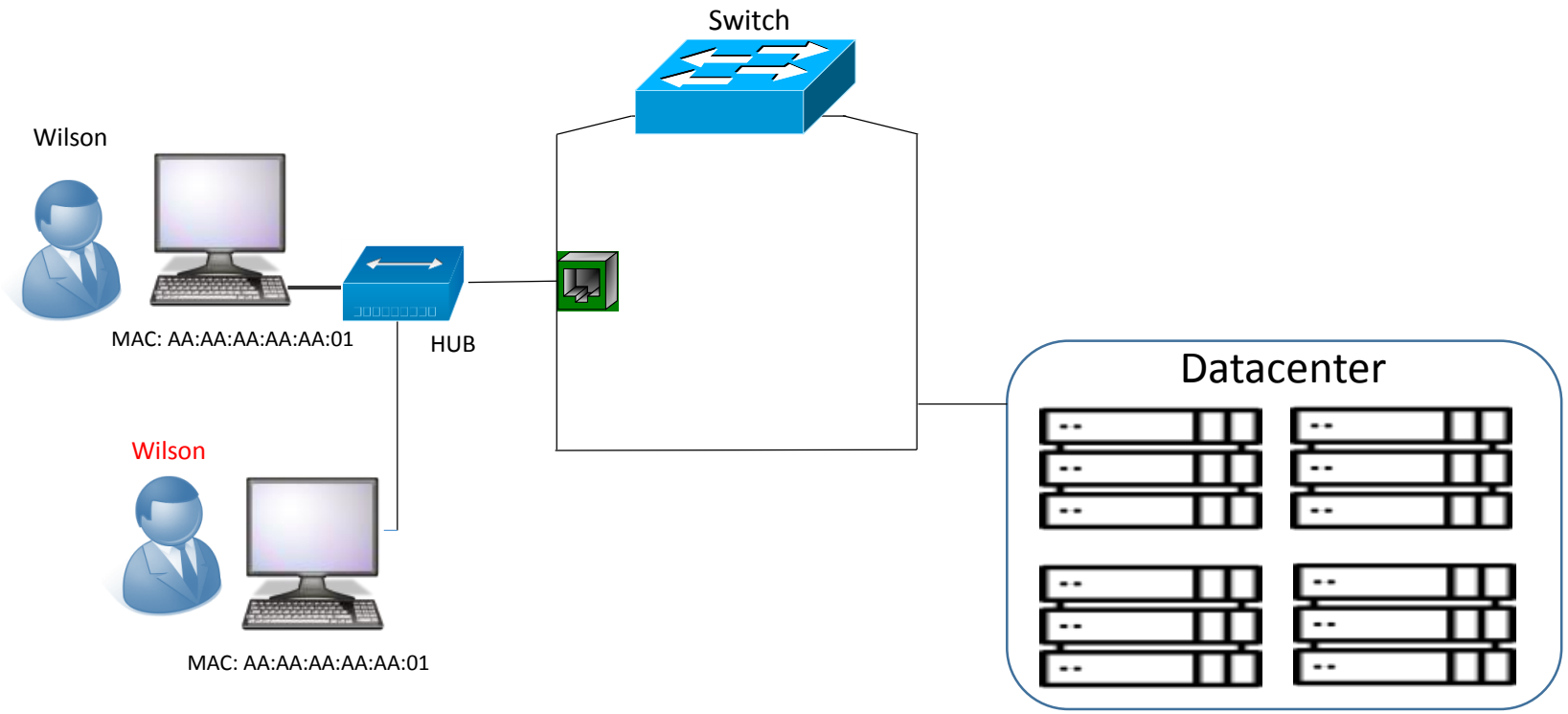
- HUB conectado na porta do switch
- Cliente autenticado
- Mac-address clonado pelo atacante
- Acesso liberado até re-autenticação ou queda do link



802.1x – Man-in-the-middle

Efetividade

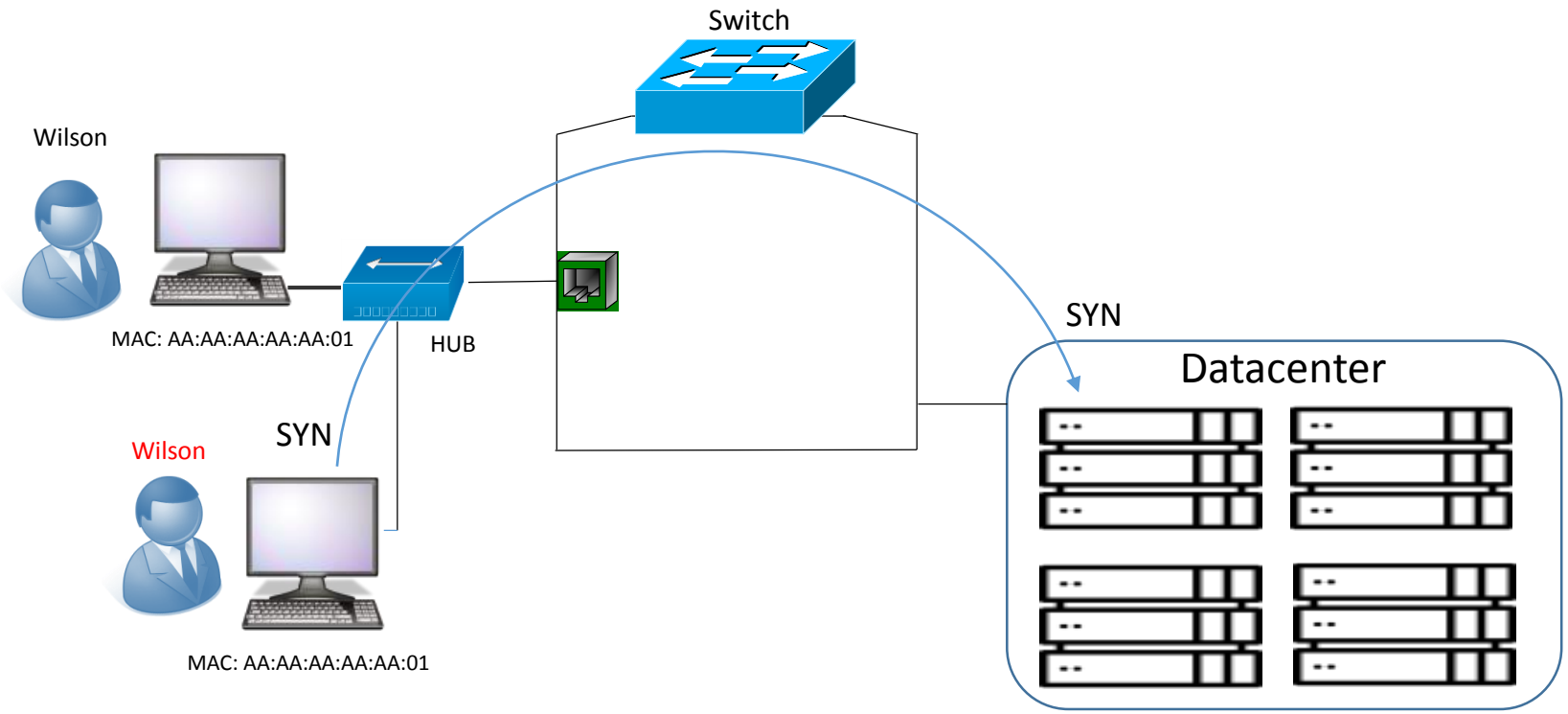
- **Desconectar endpoint autorizado - TCP race condition**



802.1x – Man-in-the-middle

Efetividade

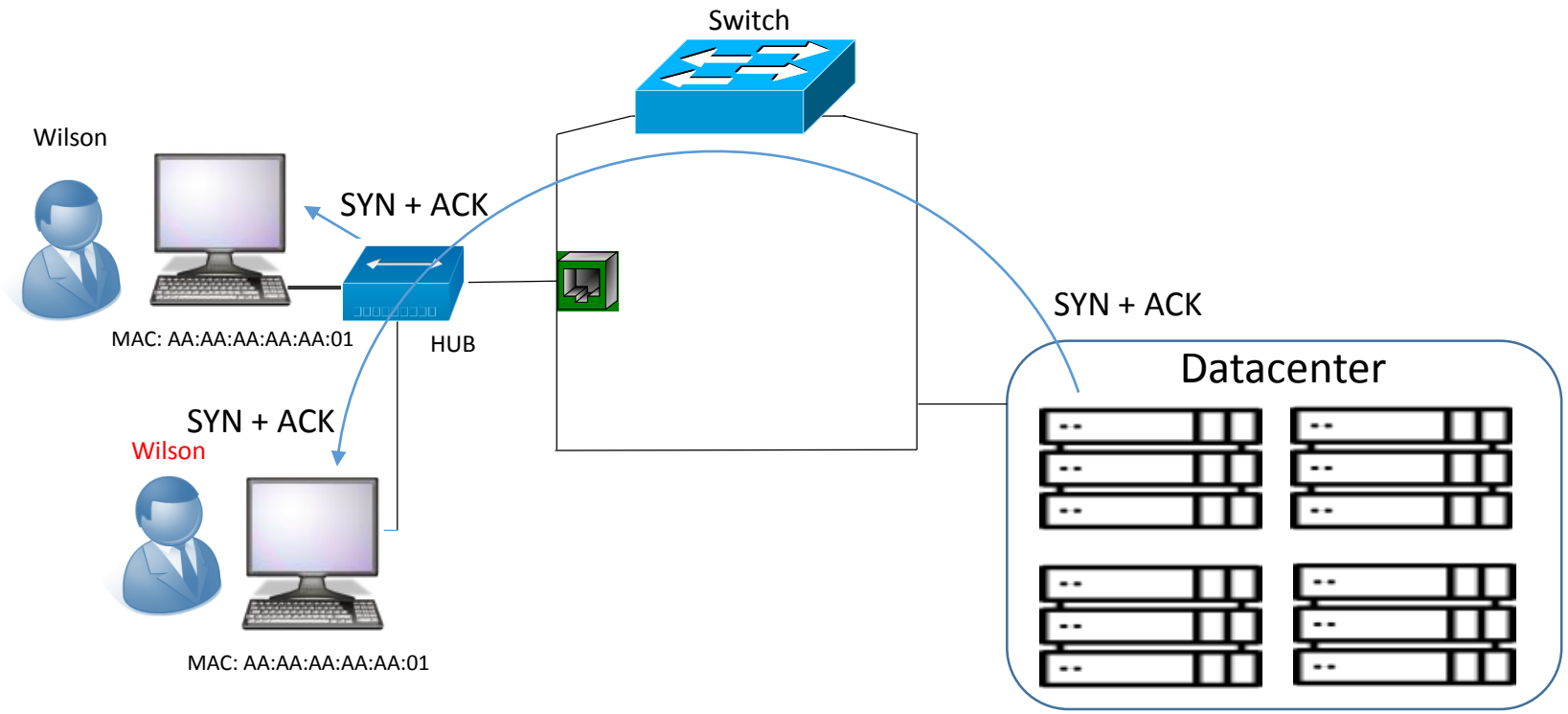
- **Desconectar endpoint autorizado - TCP race condition**



802.1x – Man-in-the-middle

Efetividade

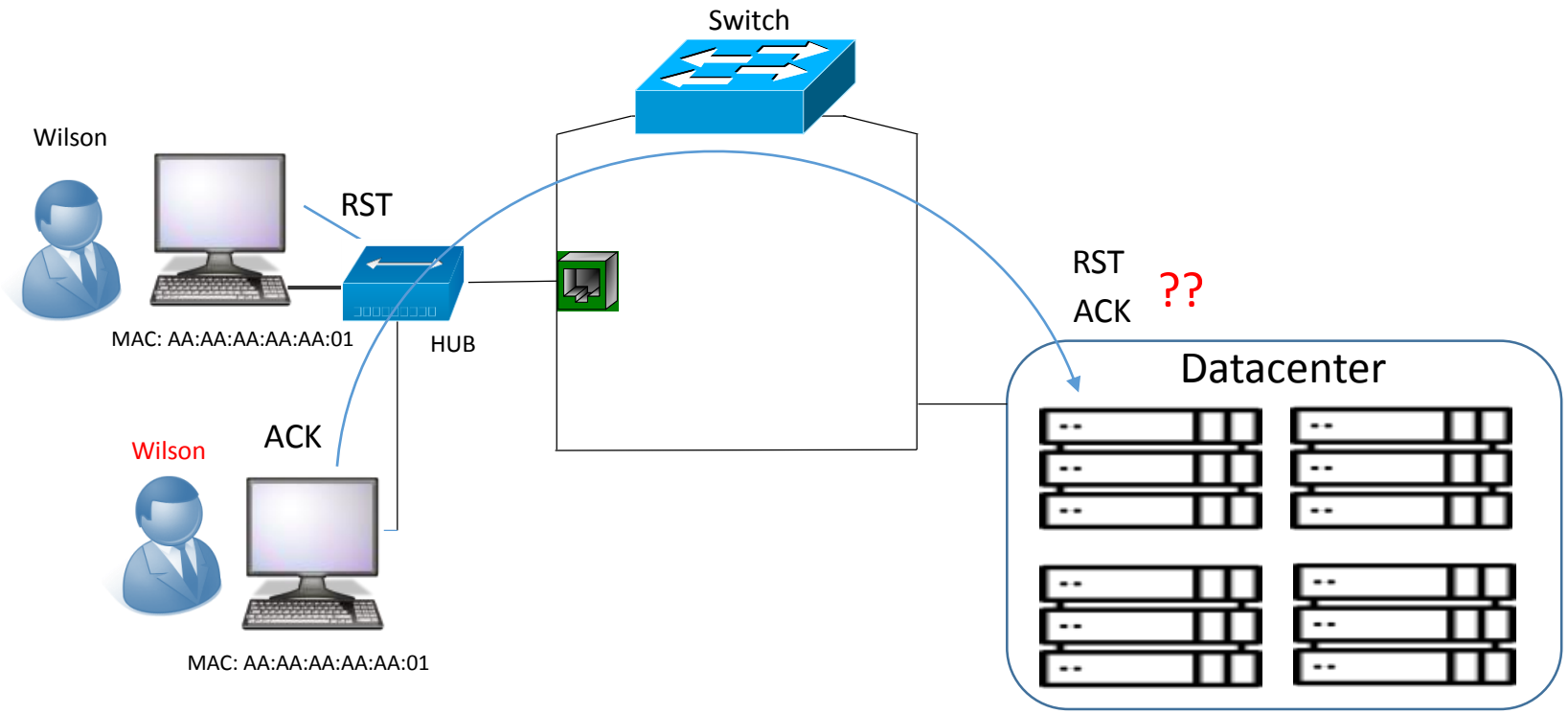
- **Desconectar endpoint autorizado - TCP race condition**



802.1x – Man-in-the-middle

Efetividade

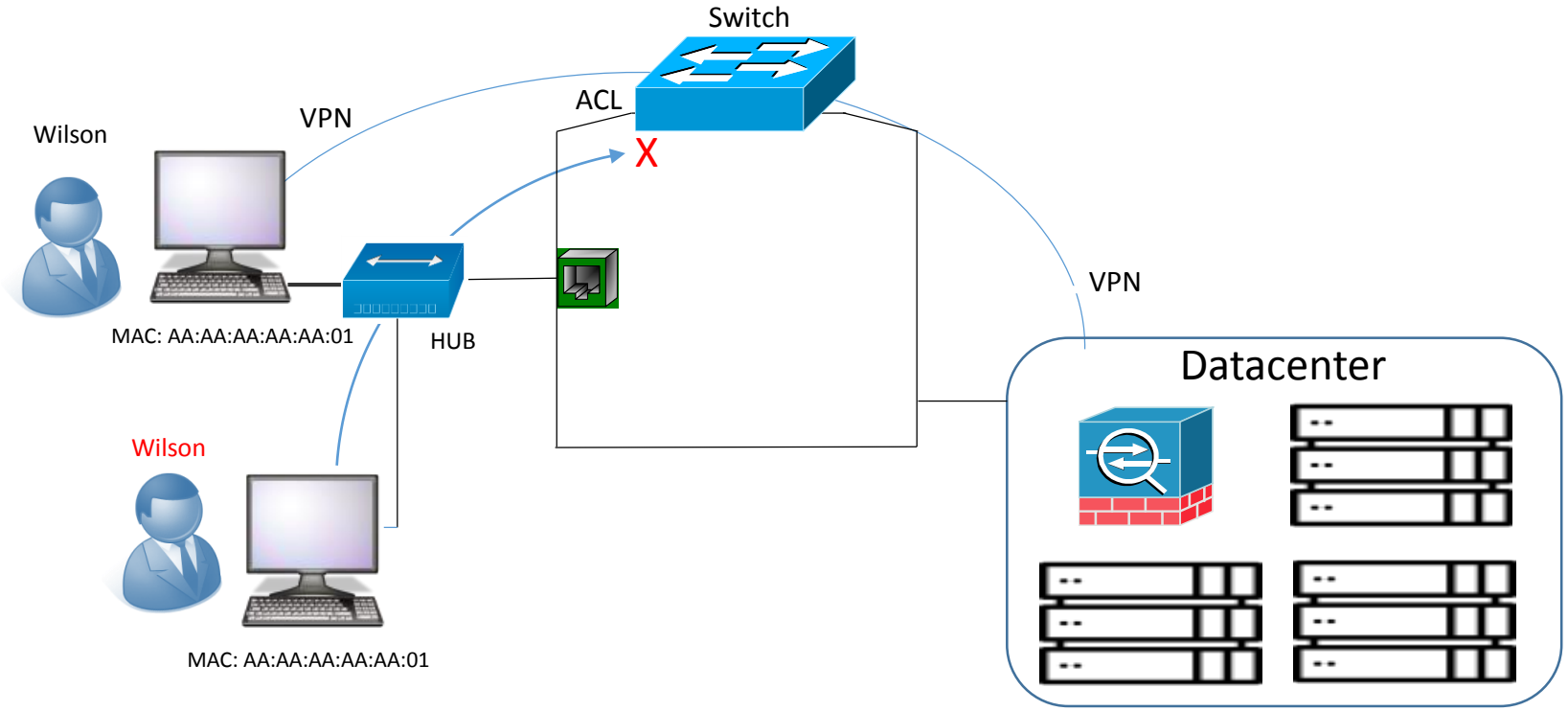
- **Desconectar endpoint autorizado - TCP race condition**



802.1x – Man-in-the-middle

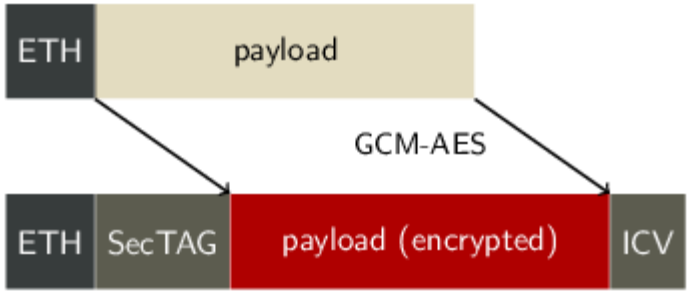
Mitigação

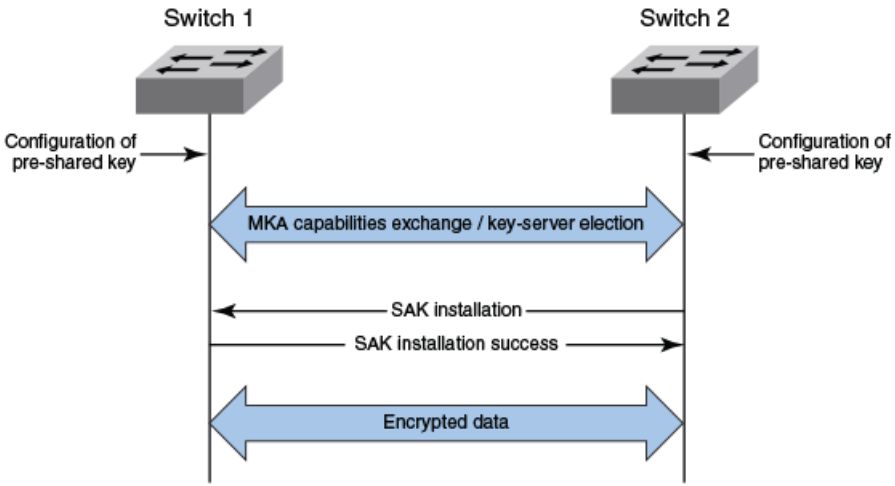
- 802.1x + VPN
- ACL no switch
- VPN only



IEEE 802.1ae - MacSec

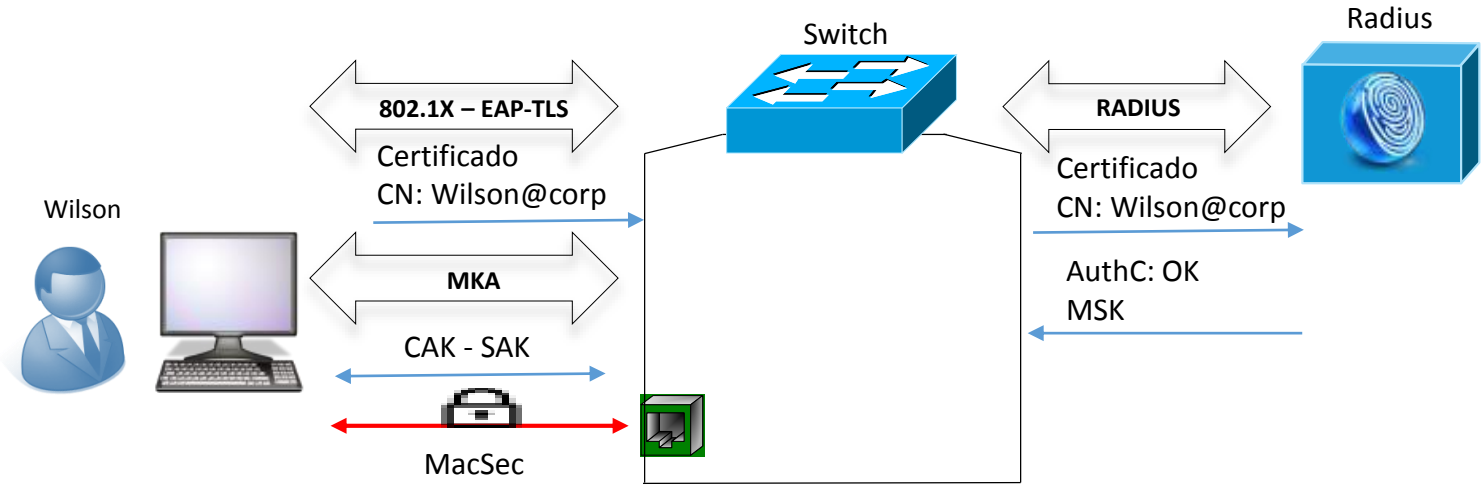
- Publicado em 2006
- Criptografia ponto-a-ponto do payload do frame
- Usado tipicamente para criptografar links lan-to-lan entre Datacenters
- Cifra padrão - GCM-AES-128
- CAK - Connectivity Association Key – pre-shared
- SAK - Secure Association Keys – derivada da CAK, trocada periodicamente
- KEK – Key Encription Key – criptografa a SAK
- Servidor de chaves é eleito para a geração da SAK





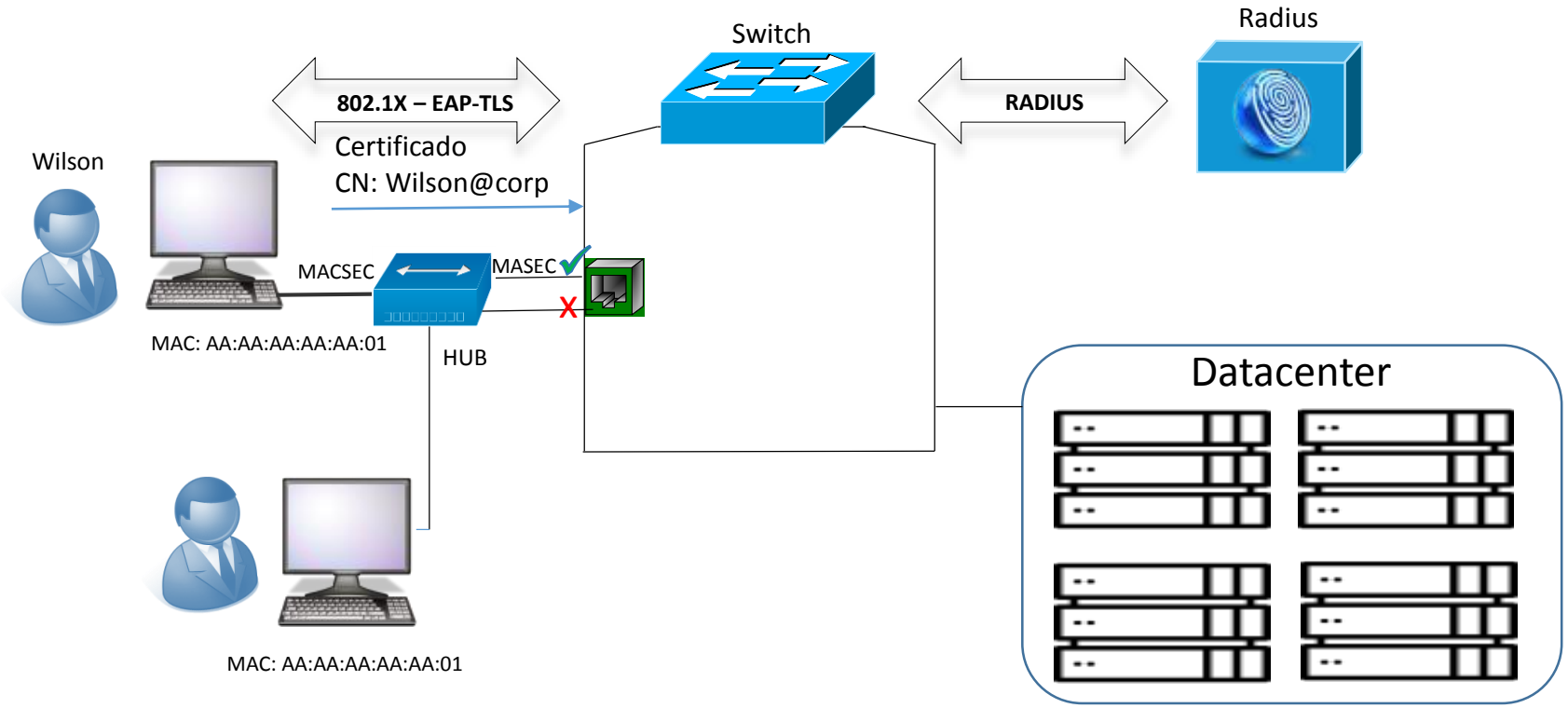
802.1x + 802.1ae

- 802.1x-2010 - EAPoL packet type 5 (EAPoL-MKA)
- MKA – MacSec Key Agreement
- Depois de autenticado, inicia-se o processo MKA
- MSK - Master Session Key – gerada na autenticação EAP pelo servidor de autenticação (Radius)
- Suplicante recebe a MSK no processo EAP
- Switch recebe a MSK em um atributo radius
- MSK usada para gerar a CAK
- Switch sempre é o servidor de chaves (SAK)



802.1x-2010

- Tráfego não 802.1ae é descartado pelo switch



802.1x-2010

Suporte

- **Suplicante**

Windows - Cisco anyconnect (NAM)
Linux – WPA supplicant

- **Autenticador (Switch)**

Cisco 3650, 3850

- **Servidor de autenticação (Radius)**

Cisco ISE
FreeRadius 2.x (à confirmar)

Referências

Identity-Based Networking Services: MAC Security
http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networking-services/deploy_guide_c17-663760.html

MACsec Switch-host Encryption with Cisco AnyConnect and ISE Configuration Example
http://www.cisco.com/c/en/us/support/docs/lan-switching/8021x/117277-config-anyconnect-00.html

MACsec: a different solution to encrypt network traffic
https://developers.redhat.com/blog/2016/10/14/macsec-a-different-solution-to-encrypt-network-traffic/

802.1X-2010 - IEEE Standard for Local and metropolitan area networks Port-Based Network Access Control
https://standards.ieee.org/findstds/standard/802.1X-2010.html